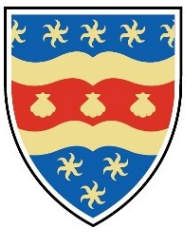
2019

Bioelectrical User Authentication

Enamamu, Timibloudi Stephen



UNIVERSITY OF
PLYMOUTH

Bioelectrical User Authentication

by

TIMIBLOUDI STEPHEN ENAMAMU

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

April 2019

Author's Declaration

At no time during the registration for the degree of *Doctor of Philosophy* has the author been registered for any other University award without prior agreement of the Doctoral College Quality sub-committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

Publications:

Enamamu, T.S., Clarke, N., Haskell-Dowland, P. and Li, F., 2017, October. Smart watch based body-temperature authentication. In *2017 International Conference on Computing Networking and Informatics (ICCNI)* (pp. 1-7). IEEE.
DOI: 10.1109/ICCNI.2017.8123790

Enamamu, T.S., Clarke, N., Haskell-Dowland, P. and Li, F., 2017, December. Transparent authentication: Utilising heart rate for user authentication. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 283-289). IEEE.
DOI: 10.23919/ICITST.2017.8356401

Word count of main body of thesis: 44,299

Signed……

Date……

Acknowledgments

First and foremost, I want to give God the glory for the completion of my PhD studies. The research project will not be made possible without the financial support and prayers of my parents Pts. and Mrs S Enamamu

I am deeply indebted to my Director of Studies, Professor Nathan Luke Clarke, for his encouraging support guidance toward the successful completion of my PhD studies. He has supported tirelessly and given inspiring advice throughout the PhD process. Thanks to the other supervisors, Dr Fudong Li for his assistance, directions and Associate Professor Paul Haskell-Dowland, who provided invaluable help and guidance throughout my PhD journey, and spent significant amount of time for proof reading research papers and my thesis.

Thanks also go to my fellow researchers within the CSCAN group (especially Mr Dany Palliyan Joy, Hind Al-Obaidi, Burhan Al-Bayati) and Umar-Faruk Abdu-Aguye for their support and interesting contributions.

Finally, I would like to thank my wife Charity Desieye, my children Favour Tari and Flourish Tonbra, Special thanks to Ebiketonmo Camron for his supportive role and other siblings Ayawari E. Okorodas, Eneboye, Prince Bibowei, Queen Amadaere Lulu-Otiede, Oyinbrakemi and Tamara-Emomoemi. Thanks also to Dr. Steve S. Ogan for a life-time inspiration, Yankee A. Owota, Vivian Datonye Horsfall and other Family members for their support and encouragement. Finally, I feel very fortunate to have so many wonderful people in my life in the United Kingdom, who inspire me and who I so much enjoy being around. Pst. And Mrs David Peters, Pst. Echika Uzoeto, Pst. Solomon & Mrs Sarah Castano, Dec. Jennifer T. Adesina, Mahmoud Alfa Abdullahi, Ubongabasi Samuel, Tola Taiwo, Ifeoluwa Grace & Peter Ekhator, Esther Efe-Aluta, Jide C. Elendu, Pst and Pst (Mrs) Abayomi Fayose and family, Dr. Ayodeji and Mrs Gbemi Adeoye, thank you for being there.

Dedication

I dedicate my dissertation work to my son Fortune Emmanuel, who was a bundle of joy to me and the family at his birth at the beginning of this research but left us for glory at the conclusion of the thesis.

Abstract

Bioelectrical User Authentication

Timibloudi Stephen Enamamu *(MSc)*

There has been tremendous growth of mobile devices, which includes mobile phones, tablets etc. in recent years. The use of mobile phone is more prevalent due to their increasing functionality and capacity. Most of the mobile phones available now are smart phones and better processing capability hence their deployment for processing large volume of information. The information contained in these smart phones need to be protected against unauthorised persons from getting hold of personal data. To verify a legitimate user before accessing the phone information, the user authentication mechanism should be robust enough to meet present security challenge. The present approach for user authentication is cumbersome and fails to consider the human factor. The point of entry mechanism is intrusive which forces users to authenticate always irrespectively of the time interval. The use of biometric is identified as a more reliable method for implementing a transparent and non-intrusive user authentication.

Transparent authentication using biometrics provides the opportunity for more convenient and secure authentication over secret-knowledge or token-based approaches. The ability to apply biometrics in a transparent manner improves the authentication security by providing a reliable way for smart phone user authentication. As such, research is required to investigate new modalities that would easily operate within the constraints of a continuous and transparent authentication system.

This thesis explores the use of bioelectrical signals and contextual information for non-intrusive approach for authenticating a user of a mobile device. From fusion of bioelectrical signals and context awareness information, three algorithms where created to discriminate

subjects with overall Equal Error Rate (EER of 3.4%, 2.04% and 0.27% respectively. Based on the analysis from the multi-algorithm implementation, a novel architecture is proposed using a multi-algorithm biometric authentication system for authentication a user of a smart phone. The framework is designed to be continuous, transparent with the application of advanced intelligence to further improve the authentication result. With the proposed framework, it removes the inconvenience of password/passphrase etc. memorability, carrying of token or capturing a biometric sample in an intrusive manner.

The framework is evaluated through simulation with the application of a voting scheme. The simulation of the voting scheme using majority voting improved to the performance of the combine algorithm (security level 2) to FRR of 22% and FAR of 0%, the Active algorithm (security level 2) to FRR of 14.33% and FAR of 0% while the Non-active algorithm (security level 3) to FRR of 10.33% and FAR of 0%.

Table of Content

List of Figure

List of Table

1. Introduction and Overview

1.1 Introduction

Authentication is a standard protection method that can be utilised to prevent an unauthorised user from gaining access to restricted information in a computing device. It is the process of confirming a person's genuine identity, a process to accept or deny the person's claim (Malempati and Mogalla, 2011 , Rao and Vedavathi, 2011). The deployment of user authentication within information systems can be traced back to the 1960s. In 1961, Fernando J. Corbato with a team at Massachusetts Institute of Technology (MIT) developed a Compatible Time Sharing System (CTSS) to avoid files being modified by unauthorised users (Feng et al., 2013, Hiscott, 2013). This has made it possible to restrict users to the portion of the system assigned to them, later passwords were used to authenticate users to access a system (Hiscott, 2013). Government establishments and leading companies have increased user authentication awareness to avert Account hijacking, Phishing attacks etc. (Rao and Vedavathi, 2011, McGregor, 2014, Morgan, 2014). There are much security concerns but there is still the need to embrace the opportunities associated with the usage of mobile application through smart mobile device for governance, business, education and social networking (Perez, 2005, PWC, 2015). With increasing cyber-attacks, implementing a stronger security mechanism to reduce or overcome them is necessary (Patil and Shimpi, 2013, Rao and Vedavathi, 2011).

The global market of Electronic Access Control Systems (EACS) (including smart phone access) is projected to reach $40 billion by 2024 (Global Andustry Analysts, 2017)

Every organisation will want to keep their internal information, document, and files from the reach of unauthorised party. The use of email and online service in organizational transactions shows that authentication is becoming more important and necessary with more interconnection of networks and advent of new technologies and services (GFI, 2009, Daya, 2013). The increase of smart devices and its usage for services means the increase of authentication burden therefore; it has become necessary to improve upon the authentication mechanism to enhance current method of user authentication. Smart phones are used for accessing e-mails, mobile banking accounts; business information etc. therefore could cost financial loss if the authentication mechanism is compromised.

The current method of user authentication that is most commonly is the use knowledge-based authentication like passwords, PINs etc. This method is popularly used for email, website account etc. Another method is the token based user authentication method, this is the used of identification cards, bank cards etc as a second layer of security. These two methods are deployed mostly because of the ease and cost of their deployment for authenticating a user (Todorvov, 2007) however they came with some issues (Gollman, 2011). To improve on the weakness of knowledge and token base user authentication, biometric is introduced to solve most issues faced by the used of the earlier methods. There has been several biometrics introduce to increase the security level of user authentication but the problem is that existing biometric user authentication methods does not solve the issue of convenience on the part of the user. Therefore, there is the need for implementing a biometric user authentication system in transparent manner to solve the issues of user's convenience

To improve on the use of biometrics for authentication, emerging biometric modalities are introduced but most of them required further work for implementing a transparent user authentication system. These include but not limited to the manner of extracting the

biometric data and how it is processed to achieve the aim of conveniently authentication a subject to access a mobile device.

1.2 Aims and Objectives

The research aim is to investigate the use of bioelectrical signals as non-intrusive method to authenticate a user of mobile device transparently. To achieve this, the following objectives are identified:

- To undertake an elaborate literature review on transparent user authentication systems and prior work on the application of bioelectrical signals for user authentication
- To undertake a technology evaluation to ascertain if an existing technology can be utilised for acquiring bioelectrical signals
- To investigate using different approaches the viability of using bioelectrical signals and contextual data for transparent user authentication
- To propose a novel architecture to support the use of bioelectrical signals and contextual data within a transparent user authentication system.
- To perform an evaluation on the proposed system to determine the overall performance of the system.

1.3 Thesis Overview

Chapter 2 of this thesis start by discussing the need for improving the authentication system as it is presently implemented. It discusses the use of user authentication system in various commercial activities. It reviewed the popularity of mobile application which has contributed to the growth of internet traffic. The chapter also discussed the use of mobile applications for E-commerce, mobile banking and others. The chapter ends with user

authentication burden with emphases on the frequency in daily login, multiple account by users, and single sign-on account used to overcome using multiple accounts with different credentials.

Chapter 3 focused biometric authentication and its use for transparent user authentication. The use of biometric has improved user authentication compared to knowledge and token base method. The use of transparent authentication has improved the use of biometric for user authentication by considering the issue of inconveniences in the process. To conclude the chapter the current state of the art in user authentication is discuss. The use of emerging modalities has further improved the way biometric is been applied to authenticate a user of a mobile device. To investigate the use of biometric for transparent authentication, the next chapter evaluate the signal for user authentication.

In chapter 4, more emphasis is place on the variability of the bioelectrical signals for user authentication and the features extracted. The most suitable wearable device is investigated from three wearable devices (smart watches). The most suitable smart watch is used for extracting the data for investigating the variability of the signal. A preliminary experiment on the heart rate is conducted using the feature selected in this chapter to verify its usefulness in application for authenticating a user of a mobile phone. With the successful use of the heart rate signal for user authentication, the next chapter extracted features from other bioelectrical signals to improve the outcome of this chapter.

Chapter 5 used the methodology from chapter 4 feature extractions to extract features from the heart rate, skin temperature and the galvanic skin response. Also, a methodology is introduced for data segmentation, data fusion, and creation of algorithm for improving the biometric performance obtained from the previous chapter. The chapter introduce the use of contextual information to improve the authentication process. One of the key tasks is the segmentation of the bioelectrical signal and contextual data into different time frames. The

time frames were applied to the bioelectrical signal and contextual data to decide the best time frame to use for the final experiment. The dataset in classified in three set of active, non-active and combine activities. Two classifiers are used for classification of the active dataset with the best chosen for the final classification of the for the non-active and combine activity dataset. The best, neural Network is used for classification of the three datasets for different time frame segments and network size. Different network sizes are used to determine the best size across the three algorithms.

After establishing the best network size that is most suitable, chapter 6 designated architecture to implement the biometric system employing bioelectrical signal with context awareness data to enhance the performance. The architecture used verities of engine and managers to achieve it aim.

Chapter 7 deals with the evaluation of the framework presented in chapter 6. The evaluation is divided into two sections with three scenarios for each section using the FRR and FAR to evaluate the framework. Chapter 8 concluded the research work with the discussion of limitation, future work from the research and the importance of the research work in general.

2. The Need for Better Security on Mobile Device

2.1 Introduction

The need for better user authentication for mobile device is desirable. This is due to the increasing use of mobile device for different services and the security implication of the information stored on it. There are different types of challenges face by the present-day user authentication system. The challenges include the burden placed on user in accessing a mobile device with knowledge-based user authentication method. The authentication burden created by frequent login of user daily is discussed with emphases on the different authentication method to solve the multiple login in this chapter. The chapter ends with a discussion on the use of bioelectrical signals for transparent user authentication base on biometric user authentication method.

2.2 Growth in Mobile Applications and Services

Research in authentication technologies is on the increase because of the exponential growth in the use of computing devices (Wallace et al., 2012). It is therefore necessary to secure these devices from identity theft, cyber espionage, data theft, cyber-attack etc. (Gemalto, 2013, Mather, 2013). The increasing computing device usage growth is mainly noticed in the use of mobile devices like smart phone, tablets for diverse activities. These activities includes quality audio and video recording, improved digital picture capturing, gaming, e-commerce, mobile applications, mobile banking, email etc. (Minto, 2012). The growth has helped in various ways to expand their usage and acceptability as means of providing services. Mobile applications have enhanced mobile services with app (application) stores established for retailing the applications for various services. This has made it easy for user to access services like online shopping (e-commerce) and banking services (e-banking) easily through their various mobile platforms. The spending on applications has increased from $29 billion to a prediction of

around $65.8 billion by 2019 (Chaffey, 2017). Beside e-commerce, banking services has also increased its services on mobile platform. Statistics shows that by the year 2019 the number of mobile phones is forecast to reach 4.6 billion. (Statistics,2018).

2.2.1 Mobile Application

Mobile applications are software designed for services deployed on a mobile device. There has been increase in the adoption of mobile application in almost every online service like banking, social networking, travels services etc. The increase in the use of mobile applications on mobile devices has greatly increase mobile web traffic because of the ease at which the online services can be accessed through these applications. In 2016, the mobile web traffic recorded 7 Exabyte per month with expected increase to 49 Exabyte each month by 2021 (Intelligence, 2017). The use of of mobile applications has also surpassed phone calls (Elish et al., 2012, Sin et al., 2012, FistOfFury, 2013). Statistics show that mobile application increased its market share from 8.32 billion US dollar in 2011 to 76.52 billion US dollars in 2017 (Dave Chaffey, *2018)*. Because of the increase in mobile applications, there is the need to secure these applications. Most mobile applications for WhatsApp, Facebook, Twitter, Skype etc. use User-ID/Password/Personal Identification Number (PIN) to secure their user's accounts (Bonneau and Preibusch, 2010, Dmitrienko et al., 2014). There are commercial authentication applications deployed to secure mobile applications from unauthorised users accessing the applications (Tarasewich, 2003). These applications include apps like Perfect App, Lock screen etc.

2.2.2 E-commerce Services

E-commerce is the use of the internet for commercial business activities through a computing/mobile device (Nanehkaran, 2013). E-commerce marketing activities are increasing to a prediction of $4.9 trillion by 2021 with mobile devices like smart phone

becoming popular platform for placing orders (Statista, 2018b). The more the internet penetrates the more e-commerce increase (*Gautam, 2014)*. The use of the internet for commercial business transaction will equally need to make payment through the internet and most of this transaction carried out through a user account. The user account will also have login details for transaction on their mobile platform that should be well secured.

The privacy and security of e-commerce will influence how users utilise online payment method because of the increasing risk of online payment (Niranjanamurthy and Chahar, 2013). Most users of e-commerce with customer account might store their account payment details on the application or web login (optional) for easy transaction when using the account. The mobile in which the application is domiciled could be vulnerable to attack, Viruses, Trojan horses, worms etc. can be used to steal user's private keys or be use in various to mislead user and intercept communication between the user and the bank (Claessens et al., 2002). This is a risk if the authentication mechanism of the mobile device is not secured enough. There are different authentication mechanisms and applications being developed with the aim of improving the security of e-commence transactions. The use of a combination of email address, user-ID or password as login credentials to authenticate a user as presently implemented by most e-commerce companies is not convenient and secure enough (Dourish et al., 2004). This is because the knowledge base user authentication used by commercial applications mostly has issue of memorability and other issues associated with knowledge base authentication.

2.2.3 Mobile Banking Services

Mobile banking services have offered e-commence a payment platform for e-commerce transaction. For the convenience of banking transactions outside the banking hall, mobile

banking has increased internet banking usage (Gemalto, 2009). In December 2011, the United States Federal Reserve board conducted a survey to investigate the usage of mobile financial services. The responses from more than 2,500 respondents shows there is an increasing range of financial services and more people utilizing mobile devices for payment (BoardofGovernors, 2014). The increase of mobile bankers over non-mobile bankers in financial transactions is increasing (*Consumer, 2015*). It is projected that by 2020, the number of people using banking services will be depending on mobile banking for payments (TechnoloJ, 2017). The projection is supported by the fact that there are mobile payment applications developed for easy mobile banking by third party developers that banking organization are adopting. This includes the likes of Paym with more than 2 million users of the application. In the United Kingdom, banks are adopting the use of Paym payment system for mobile payment transaction (Paym, 2015). The advantage of the application is the ability to perform transactions without the need of user account details but merely the user phone number (McKee, 2014). Another mobile payment application is called M-pesa developed by a German company called Paybox (Shaikh and Karjaluoto, 2015). This is a text-based mobile banking service and has been deployed in countries like Germany, Spain, Sweden, Austria, the United Kingdom and Kenya. The use of mobile payment offers an inexpensive way of banking or accessing one's account from the comfort of the home, office etc. But method is not secured enough because if the phone is stolen, transaction can easily be carried out on the phone by an impostor. Another risk associated with this text-based mobile banking method is the poor service in the communication link. The poor communication might affect the delivery of the text which is not guaranteed (Johnson and Maltz, 1996) thereby fail to carry the transaction through.

The mobile banking payment platform user authentication mechanism should accept only one person, the user to login with their account details. Mobile banking transactions can be carried out through electronic terminals at any time of the day through the web application with the use of token and with web login details. The technologies and methodologies that are used by financial institutions for online banking including mobile banking includes passwords, PIN, smart cards, One Time Password (OTP)s, USB plug-ins, tokens, digital certificates using a Public Key Infrastructure etc. (FFIEC, 2002). The use of the listed technologies and methodologies for online banking has faced some issues. It has witnessed active attacks like Trojan attack, man in the middle as well as passive attacks like password guessing, dumpster diving and shoulder surfing (Zin and Yunos, 2005). These attacks are vulnerable to secret knowledge authentication and most of the mobile banking applications make use of secret knowledge authentication method for mobile banking.

2.3 Mobile Device User Frequent login Burden

The frequency at which users access their phone daily will equally mean multiple authentications whenever the user tried to access the phone. With this burden, users of the authentication mechanism will want to increase the length of the logout time. The increase of the logout time also increases the chance of unauthorized person accessing the phone. The use of a user authentication credentials over a long period of time also compromised the authentication system. Therefore, for best practice organizations ask their customers to change their log-in details over a period of time to reduce the chance of compromising the security of the system (Pinola, 2012). While this action will increase the security; the frequent change of log-in details will also increase the burden on users. Therefore, user will want to use the same credentials for multiple accounts. For instance, it is expected that users remember their log-in details for different accounts. To reduce this burden, users

tend to use a single login detail for multiple accounts. This reduces memorability issues of having to remember the different accounts details but this is also risky (Van Der Horst and Seamons, 2007, Duggan et al., 2012). A compromised of an account means all the other accounts will face the same problem.

2.3.1 Frequency in Daily User Log-in

The frequency of authentication is defined as the "*actions performed by a single user using the same credential over a defined period of time*" (Just 2014, p.1). With a single user owning multiple accounts it is expected that users will have to authenticate multiple times a day (Scott, 2014). In a study conducted in a hospital environment, it was revealed that the frequency of log-in and log-out of a computing system to authenticate users is a source of many usability problems (Bardram et al., 2007). It brings about frustration, discomfort and can lead to the use of simple log-in credentials, long log-out time or do away with it (Florêncio et al., 2007, Pinola, 2012, Riva et al., 2012). This is the same for mobile device users. The frequency of a user log-in depends on the number of times messages, emails alerts etc. is received. It also includes the number of times the user login to perform one task or the other like making calls. A research shows an average mobile user touches his/her phone about 2,600 times a day (Zolna, 2016). This could be attributed to rise in the use of mobile application to access sites like Facebook, twitter, WhatsApp etc. with smart phone. Taking a personal experience into account, an average daily frequency of 7-10 times per hour to access messages and information on my mobile phone, therefore, users with messaging and social network app are expected to triple the figure to 21-30 time per hour therefore an average of 168 – 240 time a day to re-login into the mobile device after it is logged out. When a user login to use the mobile device, it remains unlocked if it is active. As stated earlier, an unauthorised subject can take advantage of it to have access to

the device if it remains unlocked for a long duration (Vasiete et al., 2014). To improve on this, it is better using a limited log-out time to reduce the risk of unauthorised person accessing it. The use of short log-out duration will require the user to be actively involved to login again. This will cause discomfort because it can force them away from their main task to enter a login detail (Vasiete et al., 2014).

2.3.2 Multiple Accounts by User

The proliferation of mobile applications has seen a rise in web traffic because of the ease at which web sites can be access by the click of an application on the mobile device. This has also increased the number of account created to access these applications because most online services come with user's account (Gouda et al., 2015). Florencio and Herley (2007) conducted a study to estimate the number of accounts an average user has. The study used the number of times a password is used per web sites to estimate the average account a user has. It shows that an average user has 25 different login details. This is due to the rules set by the different web sites on how to create accounts. The different web sites set the rules on the number of alphabets, numbers, signs, upper or lower case to use in creating an account. This has created an issue of memorability for the users because the usage of multiple accounts means each web site credential will have to be remembered to access the site.

2.3.3 Single Sign-On (SSO) Account

The use of multiple accounts has created a burden for a user with multiple mobile applications on the mobile phone hence the need for a single login account for multiple accounts. It will be challenging to use different credentials for different accounts created because keeping memory of them is not easy. Therefore, users might want to reduce the number login credentials by using a single login detail for multiple accounts. Also some

users do not want to change their login details periodically (as it is expected of them) for a reason of not forgetting any new login used in place of the old or run out of what detail to use for login (Cryptosmith, 2002). This also applied to mobile phones users therefore, the need to solve the issue of having to remember multiple account details for accessing the different accounts.

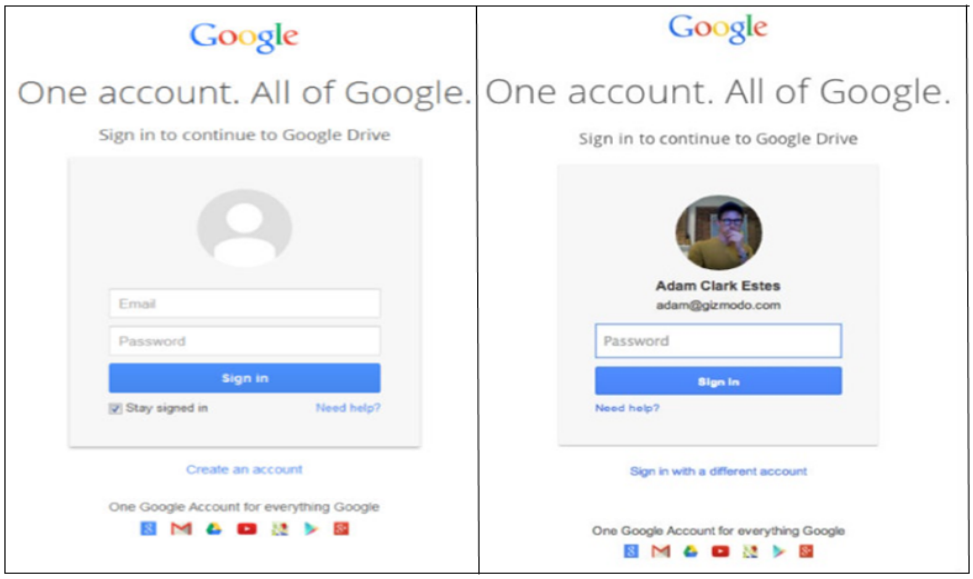
Single Sign-On (SSO) is the use of one user authentication credential for multiple-access. That is, having sign into one account; other account linked to the SSO account can be accessed using the same login detail. This is becoming popular with more users adopting the method to reduce creating new log-in detail. The use of web SSO mechanism reduces the burden of having multiple credentials for multiple website and SSO is regarded a one of the solutions for managing access to user with multiple apps and login account as website increases (Technology.org., 2017). SSO system like Kerberos has been in existence for many years now but only recently it has been commercially deployed by some web technology companies as a user authentication method for the accessing multiple websites. The SSO application used by popular web-based organizations includes OpenID, OAthen, Facebook connect etc. OpenID is a popular SSO mechanism used by companies including Facebook (before it changed to Facebook connect), Yahoo and Basecamp to prove "who we say we are".

Facebook is populated with millions of users in almost every country of the world with few exceptions (e.g. China). In March 25, 2014 at F8 development conference, CEO Mark Zuckerberg announced that users can now sign into a third party app using Facebook Connect for authentication (Welch, 2014). OAthen is another SSO used by Google, Twitter, GitHub and others. Google is a multinational Internet service corporation with a search engine that dominates 65.6% of United State market. With services like Gmail,

Google Drive, YouTube etc. it could login to those accounts with a single login credentials. Google migrated to login OAuth 2.0 from OpenID connect and OAuth 1.0.

The Twitter user base as at October 2017 was 330 million active users from 100 million in September 2011. Therefore, it has a good market share to log user into different application accounts. GitHub is another organisation using the OAthen for a community of programmers. The organisation is a programmer's social network site for code sharing and publishing. It is a Git repository services hosting service (Command line tool) with a user base of 24 million developers as at 2017 working across 67 million repositories (GitHub, 2017).

The adoption of OpenID, OAthen and other SSO for a federated user authentication has come with security issues (Hackett and Hawkey, 2012). One of the issues includes a tricky phishing scam with a title "Document" which directs one to a look-alike Google login as illustrated in Figure 2.10.



Source: ***Estes, 2014***

2. 1 : A real user and a fake (with user details) user login

It was also noticed that Google's Android operating system has some flaws that allow impostor to hijack a mobile device (Lawrence, 2014). This vulnerability was reported by Bluebox chief technologist with this statement "*The fundamental problem is simply that Android doesn't verify any claims regarding if one's identity is related to another person identity*" (Kelion, 2014). Although Google upgrading from OAuth 1.0 to OAuth 2.0, it still had some of these issues with the new login.

The migrated for Facebook SSO from OpenID to Facebook connect did not come without an issue. The SSO had a replay and masquerade attack issues which an intruder could gain access to the authorise information (Miculan and Urban, 2011). This could lead to unauthorised person accessing as many accounts that is associated with the login credentials.

In as much as SSO solves usability issues by using one memorable word or phrase to access multiple accounts. The fact is that it faces the same issues as discussed about the venerability of knowledge-based authentication method. A compromise of the account

detail compromises other accounts that are associated with it. Therefore, it has a great risk to millions of accounts as it is not secure enough to meet the present security challenges using knowledge-based authentication methods.

2.4 Mobile Device Security Issues: User Authentication

The increasing use of mobile device for diverse personal, business etc activities creates a risk if the device is not well protected. This is because the user authentication mechanism is the first line of protection of the device to unauthorised person accessing the information contained in the device. Passwords and PINs have popularly used to unlock mobile devices, but this has an issue of memorability if complex passwords are used. People want to use short and simple passwords, so they can remember it if they do not want to write it down or store on their phones. PINs are well known to be used on mobile devices when the devices are switched on (Todorov, 2007, Gehalot, 2013) and sometimes it is implemented to ask for a PIN if inactive for a specific period of time (Braz and Robert, 2006, Li et al., 2010). PINs has the same characteristics as password so faces the same issues (Zibran, 2012). The use of PINs and passwords are common and easy to implement but could be easily compromised by an unauthorized person having knowledge of it if the account owner write it down somewhere etc. as mentioned before. With the aim of improving the usability of knowledge-based method like PINs and Passwords, picture, pattern and graphic passwords are introduced. This is to solve the issue of memorability but they are easy to attack too (Faumia et al., 2014). Pictures/Graphic methods is a recognition and recall based techniques but patterns on the other hand are predefined order which the user follows to be authenticated (Sathish et al., 2013). The use of pattern comes with the same vulnerability as graphic or picture base method. Though the issue of memorability for graphic and picture password is solved to an extent, the use of

complicated pattern can lead to memorability issues while use of simple pattern can be guessed through shoulder surfing. In solving the memorability issues in knowledge-based authentication, the security of the authentication mechanism should be of more priority not to compromised user information.

2.5 Conclusion

The need to have a better authentication mechanism is not in doubt as examine in this chapter. There is increasing growth in mobile applications and services which mean more information will be accessed and stored on our mobile device. Therefore, to secure the information associated with the mobile device, there is the need for a more convenient way of authenticating a user to access the phone. Though Knowledge based authentication is still widely used but the inconvenience of accessing an account with password, PIN, image or pattern is critical because they are intrusive (Lin et al., 2013) and will require user direct action whenever knowledge base authentication is used (Takada and Koike, 2003, Campisi et al., 2009a). The time it takes to replace accounts login details periodically if a user has many accounts is inconvenient. It will also be more convenient to re-authentication periodically after a login to reduce impostor having access to the device. The use of knowledge and token base user authentication to re-authenticate periodically will be inconvenience because it means presenting the credentials periodically. Most user authentication mechanisms in use presently only verify the user at the time of login but remain open to anyone even when the device is misplaced, lost or stolen a few minutes after the user has performed a task on it if the logout duration is long. It is expected that the security mechanism of a mobile device must be robust and adapt to different environments (Nag et al., 2014). The use of biometrics improves the level of security but the point of entry to start authentication process is still intrusive to the user (Saevanee,

2014) but with emerging biometric for authentication improves usability and has more possibilities for non-intrusive mechanism (Clarke and Furnell, 2005). It has a higher probability of the user's presence during authentication therefore reduces impersonation and identity theft (Tripathi, 2011). The emerging biometric can be utilized for implementation transparent user authentication. The next chapter will present and discuss biometric user authentication in detail and its use for transparent user authentication.

3. Biometric and Transparent Authentication

3.1 User Authentication Method

With the growth of mobile applications and services, it is expected that the device that host these applications and services should be secure enough not to compromise personal information on the devices. Therefore, the credentials to access the applications and services should be unique to the user. User authentication should authorise only a genuine subject (owner of the device) to access the mobile device. The authentication mechanism of mobile devices like mobile phones, tablets etc. are mostly to authenticate a single user at a time for a device (Sethi et al., 2011). Therefore, using a personal unique identifier to log-in the authorised user is important. To improve the security mechanism of a mobile device login, the device user authentication mechanism should be as important as the usability of the mechanism to protect the stored information on the device. To improve the user authentication system, methods have been proposed which factors the log-in security and usability of the system but in solving one the other seem to be affected (Kainda et al., 2010). This can be seen in the different user authentication implementations. User authentication is implemented using three basic approaches of knowledge, token and biometric based methods.

3.1.1 Knowledge Based Authentication Method

Knowledge based authentication techniques is the most widely used authentication method because it is easy to implement. The implementation does not require additional hardware other than the device in which it is implemented (Khan et al, 2011). Based upon "certain criteria", the knowledge-based authentication methods can be divided into static and dynamic modes; static mode refers to a shared secret word like questions that is commonly used in financial institutions like 'where did you meet your spouse' etc. It is used to

identify users mostly if they forget their login details while dynamic mode is used to initiate a process of identifying a user like the persons' name, date of birth, address etc. (Nemoto et al., 2011). Knowledge based methods include Password/Passphrase, PIN, Patterns, and Pictures/Graphic methods. Password/passphrase is a universally acceptable means of restricting access into most types of account for emails, online banking, social and dating online services (Florencio and Herley, 2007). Despite a number of well-known security issues, the conventional password is the most used knowledge based authentication method because of its simple end-user authentication mechanism (Todorvov, 2007, Yazdanifard et al., 2011, Gehalot, 2013, Krol et al., 2015). The use of password or passphrase does not prove the person to be the right owner of the account but only prove that the person knows the secret to access the account (Gollman, 2011). It has several problems such as it can be easily attacked, guessed, eavesdropped, forgotten and written down, stolen etc. (Stajano, 2011, Cooney, 2012, Kale et al., 2013). The use of short password to secure an account is not safe because it can be easily revealed by using the brute force attack hence posing a security risk to the information it protects. When it is too short is can also be guessed or eavesdropped by someone closed when the information is being input or trying to say it to oneself. It can be forgotten when it becomes a memorability issue because it is too long. Therefore, the user can be tempted to write it down and when it is written down, a third party can have access to it.

When stronger passwords (e.g. using a mixture of lower case letters, Upper case letters Numbers Non-alphabetic characters (i.e. £,^, $, *, !) are utilised, users tend to forget the password for certain sites since some users access more than 20 sites a day (Khan and Zahid, 2010). With the aim to improve security, some sites issue random passwords, nonetheless, users find it challenging to memorise them (Cryptosmith, 2002). Emails of some sites can easily be hacked if the user authentication mechanism is not strong enough.

For instance, Hotmail users with over 10,000 accounts and Gawker media 1million users' details were stolen and leaked online in 2009 and 2010 respectively (Acunetix, 2014). The use of brute-force attacks can easily be carried out by using character sets (e.g. A to Z, 0 to 9) and computing the hash for every possible password (Hollingworth, 2014) and dictionary attack uses common words to guess what the password is (Andersson and Saedén, 2013). By utilising these methods, many attacks are made possible. A list of passwords that was mostly used in 2017 as illustrated in Table 3.1 shows most of the password are not mixture of alphabet and numeric characters but mostly made up of either alphabets or numeric characters.

Table 3. 1: Top 40 Worst Passwords of 2017

40 Top common Passwords of 2017							
Rank	**Password**	**Rank**	**Password**	**Rank**	**Password**	**Rank**	**Password**
1	123456	**11**	admin	**21**	hello	31	robert
2	password	**12**	welcome	**22**	freedom	32	matthew
3	12345678	**13**	monkey	**23**	whatever	33	jordan
4	qwerty	**14**	login	**24**	qazwsx	34	asshole
5	12345	**15**	abc123	**25**	trustno1	35	daniel
6	123456789	**16**	starwars	**26**	654321	36	andrew
7	letmetin	**17**	123123	**27**	jordan23	37	lakers
8	1234567	**18**	dragon	**28**	harley	38	andrea
9	football	**19**	passw0rd	**29**	password1	39	buster
10	iloveyou	**20**	master	**30**	1234	40	joshua

Source: SplashData 2018

PIN and alphabets are used in Automated Teller Machine (ATM) with ATM cards as a two-factor authentication method. The use of ATM card in addition to PIN increases the security level of the system but fraudsters have devised different ways of breaching the security. The various forms of fraud include ATM card skimming which is an issue in the use of ATM.

3.1.2 Token Based Method

Token based technique is "the use of something you have" to authenticate a user. The token can be a credit card, smart card, an ID card, a driver's license, mobile phone's subscriber identification module (SIM) etc. It is used to strengthen user authentication (Hallsteinsen and Jorstad, 2007, Tanvi et al., 2011). A two-factor authentication method is the use of a combination of something we have and either something we know (knowledge base) or something we have (biometric) (Bhattacharyya et al., 2009, Gafurov, 2010). The use of knowledge based methods like personal identification number with token reduces the memory load of using a two-step authentication of only knowledge based method (Sasse, 2005). It attempts to solve the weakness of static knowledge base authentication method (Grand, 2001) but it is relatively more expensive in implementation (Tanvi et al., 2011). The used of token increases burden by carrying a token around (Sathish et al., 2013). The use of token does not solve the problem faced when using knowledge based authentication because token can be stolen, attacked (Grand, 2001); They can be misplaced or forgotten at home, office etc. which will require it to be recovered or obtaining a new one before authentication can be carried through (Jain et al., 1998). For example, if a person forgot to carry a token for log-in into an account, it will not be easily retrieved unlike password or PIN with a second layer of memorable questions to retrieve a password. It will be frustrating if the mobile phone is used as a token is misplaced, it will becomes easier for the fraudster to access the account if the phone can be accessed (Winfrasoft, 2014).

3.1.3 Biometric Based Method

Biometric user authentication make use of various human characteristics including face, finger print, voice, iris, for authentication a person to access a mobile device (Tripathi,

2011). The use of biometric for user authentication brings benefit with respect to usability (Krupp et al., 2013). Biometric characteristic cannot be passed to another person; they cannot be forgotten, lost, misplaced or left at home, in the office etc. as in the case of knowledge and token based authentication. The acceptance of biometric is increasing but some users find biometric systems intrusive or invasive (Ríha and Matyáš, 2000). Some do not like to touch something that is used by many while some do not like their photograph taken. For traditional or religion purpose some cover their face so it becomes difficult to use the face for biometric authentication (Ríha and Matyáš, 2000). With the increase of technology and electronic devices, new opportunities are emerging in biometric for user authentication (Gafurov, 2010). This is because a single biometric method is not ideal or suited for all scenarios (Rodwell et al., 2007) so new biometric (emerging biometric) modalities are been looked at with the possibilities of their usage for better, easier security mechanism. The emerging biometrics use different physiological and behavioural characteristics for user authentication system. Some of these emerging biometric include retina recognition, gait, ear recognition, skin temperature, body odour etc. The emerging biometrics is mostly deployed for mobile phone user authentication system. The implementation of biometric user authentication system using emerging biometric on mobile phone is cheaper and easier compared to other biometrics like finger prints, face prints etc. It can be used for non-intrusive user authentication to overcome user authentication issues like frequency of log-in and other user authentication burdens.

3.2 Biometrics User Authentication System

After establishing the fact that there is the need to improve the user authentication methods as presently implemented, this chapter further describe user authentication systems, their structure and usage to authenticate a user transparently. Biometrics is defined as *'any measurable, robust, distinctive physical characteristic or personal trait that can be used to*

identify, or verify the claimed identity of an individual' (Mansfield, 1999). Biometric user authentication system can use either physiological or behavioural characteristics through automated system to identify a user (Clarke, 2011b, Tripathi, 2011, Singh and Thakur, 2012, Kaur and Verma, 2014, Nafis, 2014). Physiological authentication method measures a part of a person's body for automated user authentication following a general process of extraction, comparison and identification (Singh and Thakur, 2012). Fingerprint, facial scan, iris-scan, hand geometry and retina scan are physiological modalities which are more stable than behavioural method because they cannot be alterable except for damage to that part of the body measured (varchol and levicky, 2007). Behavioural modalities on the other hand applies behavioural pattern like voice, gaits, keystroke signature etc. to authenticate user (Wayman et al., 2005, Rodwell et al., 2007). Behavioural modalities performance can be influenced by a person's fitness at the time of verification or identification (varchol and levicky, 2007). A biometric authentication system operates in two forms, as verification and identification (Weicheng et al., 1997, Weicheng and Khanna, 1997, BenAbdelkader et al., 2002, Zargarzadeh and Maghooli, 2013). Verification to say "you are the person you claim", it is a compared claim of what is presented with what is stored as a template (1:1) while identification is against many templates stored (1:N) (Xiaomin et al., 2011). The use of biometric in authentication has been for hundreds of years through physical descriptions or the use of one's face or voice to recognise the person (Clarke et al., 2002). Fingerprint recognition, face recognition, voice recognition, iris and retinal scan and signature recognition are among the widely available biometric authentication system with more research to improve on them for user authentication (Jain et al., 2000). Other new biometrics researched on user authentication includes gait, body odour, heart rate and brain wave etc. (Wayman et al., 2005). The use of biometric for user authentication has been made easier because recent mobile devices are

fitted with sensors which enhances user authentication research (Ritchie et al., 2014). With emerging biometric modalities, organisations are looking toward employing them for biometrics for user authentication system to improve customer's satisfaction and trust (Jain et al., 2000).

3.2.1 Introduction

The use of biometric traits for user authentication is increasing because of their advantages of reliability, usability, accuracy, friendliness and security (Cimato et al., 2008). The use of a single or multiple biometric for user authentication depends on the security requirement of the system. The use of multiple biometric increases the security level of the system over use of a single biometric. To implement a biometric user authentication system for mobile device like mobile phone, features are extracted from the biometric samples to implement the system. The sample features etc. from multiple biometric are fused together depending on the implementation strategy. The performance measurement is done with respect to the acceptance of genuine user while rejecting an impostor from access the device.

3.2.2 Biometric Authentication Architecture

A biometric authentication system has a generic architecture that is made up of subsystems and components as shown in Figure 3.1. Authentication subsystems and components include data collection, feature extraction, matching, decision, storage etc. (Rila and Mitchell, 2003, de Luis-García et al., 2003, Wayman et al., 2005, El-Abed and Charrier, 2012, Chiou, 2013).

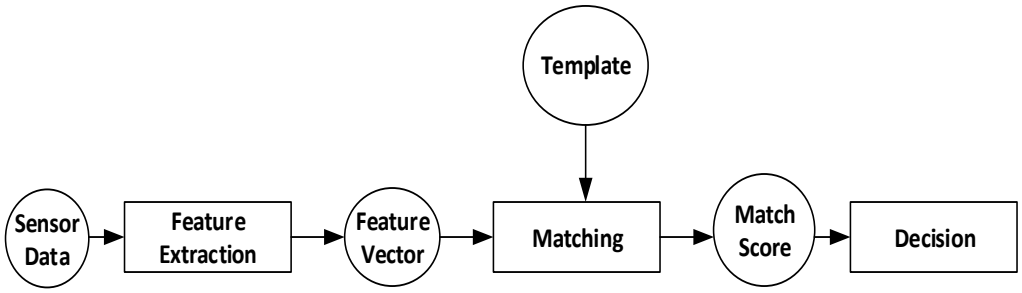


Figure 3. Error! No text of specified style in document.**.1: A general flowchart for biometric authentication**

- **Data Collection Subsystem**

The data collection subsystem collects the biometric signal, image etc. which has to be of good quality and quantity sufficient enough for accurate identification of a subject the data is collected from (Gehalot, 2013). Sensors in mobile device facilitate the extraction of data with the data collected containing some biometric characteristic that can be used for a biometric sample (Chiou, 2013, Avila et al., 2014).

- **Signal Processing Subsystem**

The data collected are in their raw form, therefore, may need further pre-processing. The subsystem does some other functions like segmentation, feature extraction, and quality control (Wayman et al., 2005, Avila et al., 2014). This can be achieved through processes such as Gaussian smoothing, histogram equalization, normalization, binarization, opening, thinning repair, and feature point retrieval (Chiou, 2013).

- **Database/Storage Subsystem**

The Database/Storage subsystem is where every processed data after enrolment is kept with details of the user associated with the template (Avila et al., 2014). This module sets the systems' policy to meet a need like having a decentralised or centralised data base. The subsystem stores the information based on certain rules created for easy retrieving of required information.

- **Matching Subsystem**

Matching subsystem encapsulates a module that decides the identity of the presenter of a captured data by comparing it with the stored template. The matching subsystem acts by presenting the sample captured and the stored one if it is for verification of a single template while comparing it against all possible samples within the system for identification of subjects (Avila et al., 2014).

- **Decision Subsystem**

The decision subsystem makes the decision of accepting the user or rejects it by determining if the presented data matches or does not match the stored template (Gafurov, 2010, El-Abed and Charrier, 2012, biomtrics, 2014). There are two outcomes for either a genuine or a false individual presenting his/her biometric details. They are either a genuine individual is accepted or rejected or a false individual is accepted or reject depending on the threshold settings (Avila et al., 2014).

3.2.3 Biometric Trait Quality

The used of biometric trait for user authentication has its pros and cons therefore, the characteristic of the biometric trait should be of quality. There are qualities that is required when selection a biometric trait for biometric application for authenticating a subject. The biometric modalities should have high performance for the indented application and should be accurate to a required degree. These qualities are listed as:

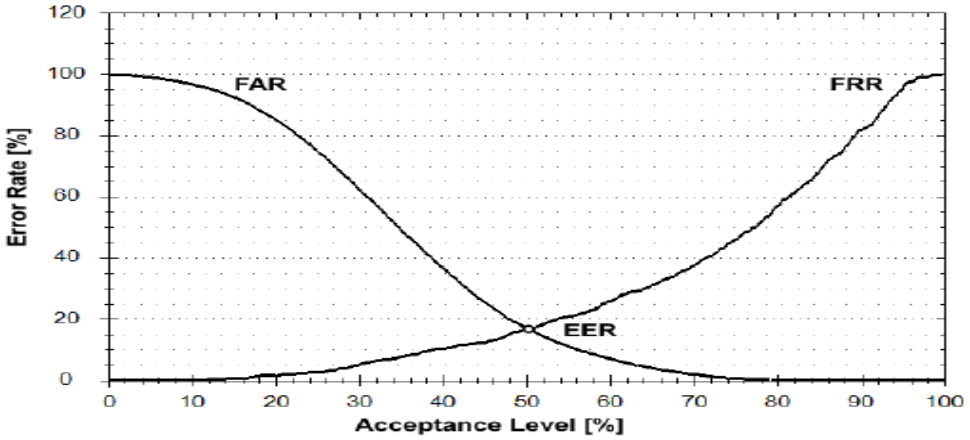
- **Universality:** All subjects used for the biometric authentication should have the same biometric trait required.
- **Uniqueness:** The biometric trait should be sufficient enough to discriminate the subjects.
- **Permanence:** The biometric trait should be stable over a significant period.
- **Measurability:** The biometric trait should be easily acquired using a suitable sensor or device.
- **Performance:** The recognition accuracy should meet the requirement of the application for used.

- **Acceptability:** The users should be willing to present the biometric trait for acquisition.
- **Circumvention:** The biometric trait should not be susceptible to mimicry or spoof attacks.

3.2.4 Authentication Performance of a Bioelectrical System

To authenticate a subject, there are parameters used to determine the criterial for accepting or rejecting a subject. A biometric system need to be measured to verify its performance. Therefore, to evaluate the performance of a bioelectrical authentication system, impostors and genuine data are used. The evaluation metric calculates the Equal Error Rate using False Accepted Rate (FAR) and False Rejection Rate (FRR) (Phillips et al., 2000, Mansfield and Wayman, 2002). The lower the EER the more accurate the system is therefore it expedient to have a lower FAR and FRR.

- *The Equal Error Rate* is the point at which the False Accepted Rate (FAR) and False Rejection Rate (FRR) meets as shown in Figure 3.2.
- *The False Accepted Rate (FAR)* is the rate at which a user that is an impostor is falsely accepted to access a system
- *The False Rejection Rate (FRR)* is the rate at which a legitimate user is falsely rejected to access a system.



Source: SYRIS, 2004

Figure 2.2: Showing the Threshold value for EER

3.2.5 Biometric System Implementation

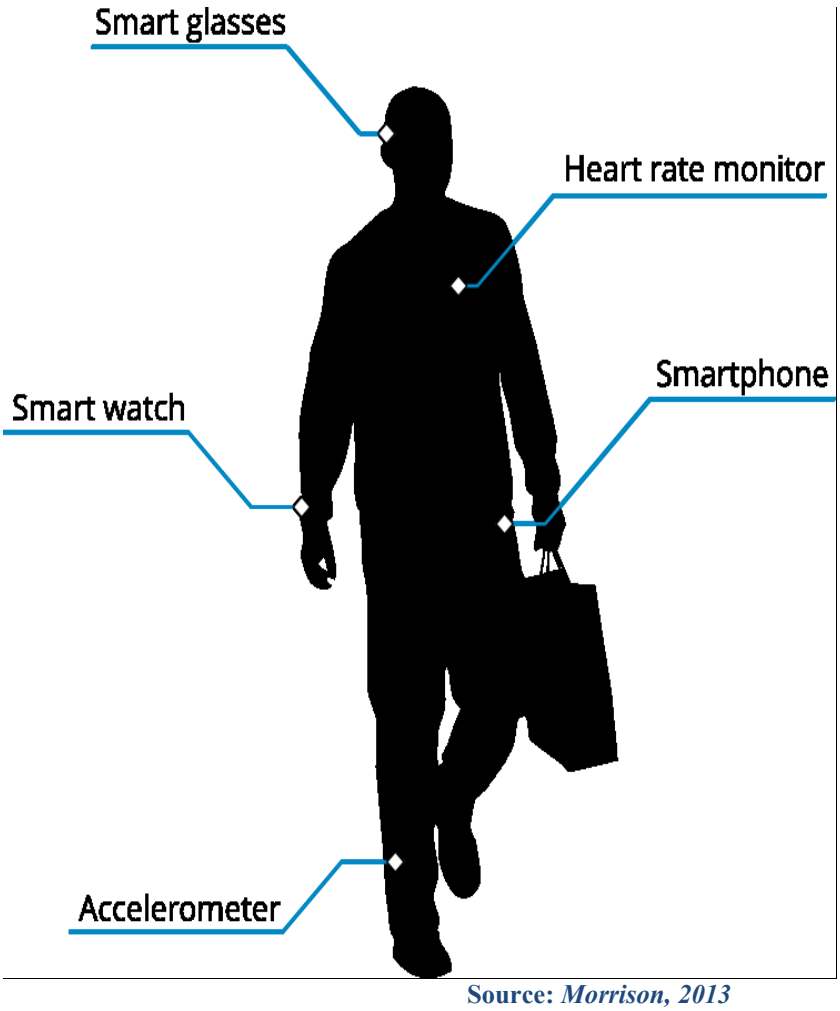
A biometric system is implemented as either unimodal or multimodal biometric system. The use of unimodal biometric (one modality) is more common in real-world implementation (Ross and Jain, 2004). Fingerprint modality has been one of the earliest method of unimodal biometric identification that is well established and widely used dating back to over 100 years (de Luis-García et al., 2003, Stephen and Reddy, 2011). Other unimodal modalities that are established include palm-print, voice-print, face recognition etc. Unimodal biometric is widely used in boarder control and voting because it is simple to implement and highly dependable for the verification. There are disadvantages associated with unimodal biometric that includes intra-class variations, inter-class similarities, non-universality etc. The use of multimodal (multiple) biometric to authenticate user increases accuracy, it also provides an option where a user does not have one of the modalities to present e.g. a finger. Thought fusion of modalities enhances user authentication performance but not every fusion contributes positively to performance

(Clarke 2014). Therefore, when fusing modalities, the modality properties should be well investigated before fusing the modalities to enhance performance.

3.2.6 Biometric for Transparent Authentication

The current standard methods for user authentication must involve the user in the authentication process. This involves the participation of the subject to be actively involved. The use of a non-transparent authentication process brings about usability issues. The user of the authentication mechanism is a constituent part of the authentication process. This is because the user must consciously interact with the device. For example, for finger biometrics the user will have to present the finger for capturing. The user must present the finger to login as many times the device log the user out. This is an issue that will force the user to used longer log-out time or do away with it as stated earlier in the chapter. Therefore, the use of active user authentication is highly desirable in today's society (Roth et al., 2014, Kaganov et al., 2014). This is essential for the future of biometric user authentication system (Nag et al., 2014). If the user authentication is not aimed to be continuous, then the aim of achieving a stronger authentication mechanism for mobile computing devices might be defeated because it brings robustness to the system (Davis, 1987). There are researches on going on the use of sensors installed in mobile phones to achieve a transparent authentication by extracting reliable biometric data for a continuous and transparent authentication (Crosby and Ikehara, 2004). Most of the wearable devices in the market presently are fitted with sensors like accelerometer and gyroscope sensors, motion control sensors, heart rate sensors, body temperature extraction sensors etc. The extracted data from sensors have the capability for implementation user authentication (Chuang, 2014). To implement a transparent user authentication, sensors with the abilities to capture user behavioural biometric activity will enhance security

without user's intrusion. For example, Biodynamic feature based on user responds to specific stimuli while performing one activity or the other, dynamic behavioural traits of user like facial expression, gesture, gaits, bioelectrical signals can be capture with dynamic wearable devices (Abe and Shinzaki, 2008). Most of the smart phones available in the market can communicate with wearable devices and sensors. With the use of wearable technology, transparent authentication can easily be implemented as they can be worn on the body as an eye glass, wrist watch, pouch-sensor etc. as illustrated in Figure. 3.4 (Morrison, 2013).



Source: *Morrison, 2013*

Figure 3. Error! No text of specified style in document..**3: Wearable sensor and garget**

3.3 Current State of the Art in Transparent Authentication

Many authentication methods applied to conveniently authenticate users of a mobile device seem to fall short of the ability to do so easily without the direct involvement of the user. The direct involvement of a user in the authentication process brings about usability issues at the point of entry as stated earlier in this chapter. The use of emerging biometric modalities seems to solve the issue of user's involvement at the point of entry. In as much as security is the major concern in designing an authentication system, usability plays important role in the use of it (Braz and Robert, 2006, Josang et al., 2007, Braz et al., 2007). To implement a transparent authentication, the system should be able to continuously extract biometric data without prior request to the user for action to extract biometric samples. The process should be done in a manner that is convenient and easy to use. Many biometric modalities have been used as either a single modality or fusion of multi-modalities to solve the issue using transparent and non-intrusive method at the entry point. The use of transparent user authentication increases the security level but it comes with its own issues too (Clarke, 2011b). One of the issues includes usability while trying to achieve a higher level of security. Many user authentication system designs are tilted more toward the security aspect of it but users are driven more toward convenience and usability of the mobile device security mechanism (Weir et al., 2009). There should be a convenient level of trade-off between usability and security in the design of a convenient user authentication system (Schultz et al., 2001, Dourish and Redmiles, 2002, Braz et al., 2007).

3.3.1 Transparent Authentication: Single Modality

There are different studies and proposal on the use of transparent method for user authentication. To evaluate the different approaches used to achieve transparent

authentication as a single or multiple modality, this section will study some selected research works on transparent authentication. The selected research works used publish papers and journals for review based on recent works (within ten years) using biometric for authentication. The authentication implemented should be based on a mobile device user authentication system with the aim of achieving it transparently.

- **Finger Print Modality**

The integration of finger print scanners started with Motorola smart phone called Motorola Antrix in 2011. After this, other companies introduced finger print sensor on their mobile phones. There are many mobile phones in the market today with fingerprint scanners for transparent authentication, they include IPhone5, HTC One Max, Samsung's Galaxy S5 (and other Galaxy family), Sony Xperia Z5, Huawei Mate etc. The introduction of finger prints on prior mobile phone did not attract much attention not until Apple incorporated finger print on its mobile phone. To improve the issue of usability, Apple in 2013 explored the used of finger print for transparent user authentication by integrating finger print scanner to the home button of iPhone 5s. To transparently authenticate the user, it is expected that the home button is used to switch on the phone. Therefore, the authentication process is done transparently as the user tried to switch on the phone. The aim is to authenticate the user only at the beginning of the process. The fingerprint allows for a quick login and prevention of unauthorised user to login at the beginning but there seem to be an issue of authentication beyond the point of entry to verify the user. After the point of entry authentication, the home button is not used to activate any other function instead the touchscreen surface is used. Few months after the release of iPhone 5s, it was reported by the chaos Computer Club in Germany that a fake finger print could be used to unlock the iphone5 (Frank, 2013).

- **Touch Screen Interaction**

(Frank et al., 2013) work goes beyond the point of entry to touch screen interaction after gaining access into the mobile device. In the proposal, he used 30 behavioural touch features (raw touchscreen logs) extracted using users populated distinct subspace of the feature space. This process is done in a continuous manner and is also transparent to the user. The Continuous Touch-Based Authentication system records the touch data as different stroke sliding horizontally over the screen (when browsing through images or moving in between icons), sliding vertically over the screen up or down (reading email, document or web pages). A proof-of-concept classification frame work was proposed to learn the touch behaviour of users which is later used to challenge the touch data being recorded as the user interact with different applications on the device. The experiment used 41 subjects with each subject spending 25-50 minutes to read through texts. The same experiment was carried a week later with a shorter time interval but limited the subjects to their preferred way of using the phone. The classification framework used two different classifiers, *k*-nearest-neighbors (*k*NN) and a Support Vector Machine (SVM) with an rbf-kannel. The researcher chooses the classifier base on its robustness and fast classification method. The classifier takes new observations that in this case, strokes and locate it in feature space with respect to the closest training observation. The later classifier is chosen because they are popular, powerful binary classifier. The choice of the number of strokes taken before classification is obtained introduces a trade-off between usability (reduction of false rejection) and its security (reduction of false acceptance). In a single stroke, the EER of each classifier is approximately 13% while using about 11 to 12 strokes the Equal Error Rate is reduced to 2% and 3% with SVM achieving a lower error than *k*NN classifier. The combination of both classifiers achieved an EER of between 0% and 4%

depending on the application scenario which give the system a robust authentication however touch-base authentication method has a security and usability issues with context and environment (Fischer et al., 2012). From research it is observed that the User Interface (UI) and the displays sizes of a mobile device, the processing speed affect the accuracy of the method (Zhao et al., 2017).

- **Keystroke Analysis**

Campisi et al. (2009) used the keypad of a smart phone as the data collection device (QWERTY keyboards). The proposal used the key down-down time and key up-up time as its base unit measurement using the mobile keypad. A single letter entered is used as a biometric sample. The research used a database containing 30 users with 3600 keystroke acquisitions. The research employed statistical classifier achieving an EER of 13%. Another researcher Kaganov et al. (2014), used a different approach but the same database. The proposed method effectively maintains all information used by the user's most recent activity. The information from the keyboard activity is stored as a single vector of fix size. The approach main idea is the construction of an empirical feature map (the resent symbols pressed by the user) that explicitly maps an arbitrary sequence of pressing/releasing symbols from the alphabet (finite alphabet) with timestamps into a finite-dimension metric space of a feature vector (times of pressing and releasing). In the proposed system, every letter typed is a vector and it contains sufficient information about the previous sequence of the user's keystroke action. A decision trees and their ensembles basic learning algorithm was used because the dependences included in the proposed feature vector structures are sufficiently nonlinear and their complexity is specific for every situation. The performance of this proposal was check using a data representation model known as dataset Si6 containing 66 sections from 62 subjects. Each subject tried 15

sessions with a pre-fixed passphrase. Another data was collected from 40 university students within two days. The first day's data was for training while the second day's data is used for testing. The time used for training and testing was for 3 hours and 6 hours respectively resulting to about 24 thousand keystrokes. The evaluation was done using all other data except for one that is used to try to gain entry. The threshold confidence level for testing was set 10 times higher than the maximum confidence level for the training level. The Si6 dataset achieved an ERR of 6% while the data collected from the student achieved an average ERR of 13%. The use of keystroke for user authentication without additional authentication layer of defence could lead to weaker authentication system. This is because keystrokes in general have lower accuracy which could be due to external factor like fatigue, distraction or injury (Wankhede and Verma, 2014).

- **Voice Recognition**

Jayamaha et al. (2008) used Hidden Markov Model (HMM) for voice print authentication which is well established for speech recognition (Bahl et al., 1994). In the proposal named '*Voizlock*', the correlation of the physiological and behavioural characteristic of the speaker is used for authentication purpose. These include how fast or slow, how loud or low the user speaks. The system took note of the fact that a user cannot be stable to put the variability into consideration. The voice print collection is done by recording the user when using the phone with the output stored as a formatted .wav file. This sample collected must be free of clipping, loud enough and with less background noise. The sample is further processed to eliminate any noise remaining. Using a voice training wizard for training, the system produces a sound for the user to reproduce. The process signal is segmented in successful frames of between 20ms and 40ms. The performance is evaluated by the number of success an imposter gets authorization by mimicking a genuine

voice (1.33% success and 98.66% failure) against success by genuine user (86.25% success and 13.75% failure). One of the drawbacks of this system is that it can be deceived by replay attack using a recorded voice (Jayamaha et al., 2008). Another drawback is the environment listed issues, avoiding clipping and noisy environment. This is because the advantage of a mobile phone is its mobility therefore, the location becomes irrelevant as along as the user and the caller can hear themselves.

- **Face Print**

Venkataramani et al. (2005) investigated the performance of face authentication. It uses three face verification algorithms of Correlation Filters, Individual PCA, and FisherFaces for the investigation. 20 subjects were used with their images taken with a phone camera. The image capturing was done in two stages and in two sets for each capturing. One set for training and the second for testing. The first image was taken in normal ambient background indoor lighting with the second image taken outdoors in different locations in two rounds. In processing the image, the distance between the eyes where used to crop the face and then contrast stretching was done to normalize the image unit energy. In the evaluation stage, three algorithms were used with a threshold set on the Peak-to-Sidelobe Ratio (PSR) for correlation filters to find the Equal Error Rate. The best average EER for correlation filters is given as indoors 1.1%, outdoor-1 is 0.8% and for outdoor-2 is 2.8% with overall average of 1.4%. For Individual PCA indoors EER is 4.1%, outdoor-1 is 5.6% and for outdoor-2 is 3.4% with overall average of 4.0% and the best average EER for FisherFaces indoors 1.0%, outdoor-1 is 1.0% and for outdoor-2 is 1.3% with overall average of 1.0%.

In another research, Kaur and Singh, (2012) aimed to strengthen and improve on the disadvantage of Social Network Site (SNS) inefficient authentication system log-in (Dietz

et al., 2012). The acquisition is done with a simple web camera using *J2EE* and *JavaScript* for upload image and up-grade personal profile, view friend list and friend request acceptance/ rejection. The system developed two categories of database, one for images captured using the web-camera when users register and the second one for the image of the user uploaded as a profile image on the social network site. Using 75 subjects, the data capturing is activated when the user presses the home page of the SNS, the web-camera automatically captures the facial image, normalize it and verify if the image is in a data base after which the login is opened. Four algorithms of Principal Component Analysis (PCA), Independent Component Analysis, Linear Discriminant Analysis (LDA) and Support Vector Machine (SVM) is used. This is based on their good performing algorithm for face recognition (Givens et al., 2004). The evaluation was carried out with the four algorithms to get the best performance. The result showed a very promising range 79.77% - 93.10% success in authenticating a genuine user with Support Vector Machine (SVM) showed the highest performance. One of the challenges in face authentication is that face changes over time or use of make-up or natural wrinkles can alter the look of a person (Tresadern et al., 2013).

- **Phone Orientation Analysis**

Tang et al. (2010) fused multiple information acquired from the phone to achieve transparent authentication using Apple phones. The proposal introduced data mining to authenticate a user by using the application history, Global Positioning System (GPS) information. It is expected that a user follows a similar daily habit therefore the training period was long enough to get a better threshold. The data are in directional graphs and a rule-based classifier is used to identify the user. The classification is divided into two classes of a genuine and negative user. During training, each user spends 15 days

collecting data for training with only positive training data collected. The testing was done using another 5 days with 10subjects. The experiment achieved an average accuracy of 76%.

Taking advantage of the features loaded in a present day smart phone, Lin et al. (2012) used the same phone orientation for user authentication. The approach is based on the behavioural pattern of the user holding and movement of his arm when using the phone. An application to collect user's behavioural pattern of the up-down and left-right flick, spread, pinch etc. was developed to capture the data from the orientation sensor. The data collection model is based on three axes of x, y, and z. using the angle around the x-axis, when the phone is tilted toward north, the compass is 0º or 360º, 90º when toward east, 180º when toward south and 270º when toward west. The angle around the y-axis, when the phone is on the flat surface facing up the angle is 0º, 180º or -180º when it is facing down. It is -90º when it is upright and 90º when it is upside down. On the z-axis, when the phone is in a rolling position it is 90º or -90º. When the screen of the phone is facing right it is 90º and -90º when facing left. If the rolling angle is 0º the phone is lying facing up. Using a Wildfire Android smart phone, the behavioural biometric was captured using 20 subjects for the experiment. The subject used the same phone to product 37,400 samples with each producing 1,800 flicks per data set. The proposal used stepwise linear regression to select good feature subset with a *K*NN used as the classifier. The evaluation was done with three performance measures: False Acceptance Rate (FAR), the False Rejection Rate (FRR), and Equal Error Rate. During evaluation, it was observed that performance rises in respect to the test sample by EER of 6.85% when the number increased to seven. The security level for point of entry of the proposal is not good enough hence the researcher recommended it for continuous verification instead of the point of entering verification. The approach can easily be fooled when the user is doing some work on it and places the

phone on a flat surface or the user is stable in a position, which can make it difficult to differentiate an unauthorised user from the genuine user.

- **Word Signature**

Clarke and Mekala (2007) evaluated the feasibility of using word signature to authenticate user of a mobile device. The work is based on the use of common words (signature) by the user and the ability of the system to differentiate a genuine user from an impostor. The study used 20 subjects with each one given two opportunities to act as the authorised user while the others act as impostors. The impostors were also given two opportunities to access the system using the authorised user's credentials. The collection of data is done with a Toshiba Pocket PC using an unmodified version PDALok to collect the data; the investigation is done in two sections. First, in a control experiment where user signed their credentials in a normal fashion and a second, a feasibility experiment where the users were given words to use. The result achieved FAR of 0% and FRR of 3.5% it showed that the feasibility experiment was better with FAR and FRR of 0 and 1.2% respectively. One of the drawbacks in word signature is that subject of the field could use common word relating to their profession when writing; this could give an impostor access the device.

- **Gait Recognition**

Nickel (2011) carried out a study using gait recognition system to authentication user on a mobile device. The system used wearable sensor, an accelerometer on the body to collect the data for the templates. The accelerometer signals are from tri-axial measured backward-forward, sideways and vertical spatial dimensions. The data is collected from user's gravity, vibration and noise recorded on the accelerometer as the user moves using a non-cycle-based gait representation. The research used 48 healthy subjects walking for

around 37 meters (as one data class) turned around and walk back (as second data class). The features are extracted from a times-series data and the sample data collected where pre-processed using feature extraction algorithm that works with consistent and portioned data. An average sample rate of about 50-40 data point per second is used. The mobile device is placed in a pouch that is attached to the body as data is collected. The data collected on the first day is used for training and data form the second day is used as the recognition pattern. A Support Vector Machines (SVM) is used as classifier to achieve a fixed length vector of discrete values. The Mel-frequency Cepstral Coefficients (MFCC) and Bark Frequency Cepstral Coefficients (BFCC) are further used. SVM classifier is used for separation of the two classes of data. The performance is calculated using a False Match Rate (FMR) and the False Non-Match Rate (FNMR). The evaluation is done in segment for different lengths and interpolation rates. The result achieved a FNMR of 59.9% and a FMR of 1.3%.

(Han and Bhanu, 2006) in an experiment carried out to improve gait based user authentication proposed a statistical feature fusion approach. It used a spatio-temporal gait representation called Gait Energy Image for the experiment (Geiger et al., 2013). The real templates were computed while the synthetic templates were generated. The experiment used USF HumanID gait database for comparison with other templates for the experiment. It divided each gallery silhouette sequence into cycle frequency and phrase estimation. A real gait template for each cycle is computed, and then distorted to get synthetic gait templates. A component and discriminant analysis are carried out for the real and synthetic gait templates and later transformed using transformation matrices to achieve real and synthetic gait features. The real and synthetic templates were separated for feature extraction. In carrying out training, two approaches for finding transformation for dimensionality reduction is used. The Principal Component Analysis (PCA) and Multiple

Discriminant Analysis (MDA) set to achieve the best class reparability simultaneously. The approach achieved a competitive performance success rate of between 97% - 100% depending on the real, synthetic and fused templates. In a real live implementation of the method, it might have phone placement issues. While gait authentication for mobile phone hold prospect because of the motion sensor like gyroscope and accelerometer, the issue it faces for implementation using a mobile device is the position the user places the phone. This might be different from the area the initial training was done. For example, if the user places the phone in a tight jeans pocket while the training is done wearing a loose trouser, this might affect the output. Also, the user is not expected to consciously place the phone in a direction or position that in turn will affect the result.

3.3.2 Transparent Authentication: Multi-Modality

The used of multimodal biometric reduces the possibility for unauthorised user to access a system (Bubeck, 2003). It was established earlier in this chapter that there are different subsystems, but three main subsystems form the fundamental subsystems. This three subsystems are where the modality fusion is implemented, these are the Data acquisition subsystem, Feature extraction subsystem and Matching subsystem (Mansfield, 1999, Stephen and Reddy, 2011). The fusion of the different biometric modalities is the key to a multimodal system (Indovina et al., 2003). Multimodal fusion increases the level of security and confidentiality compared to unimodal biometric (Nandakumar et al., 2009). It also improves some limitation found in unimodal system (Ross and Jain, 2004). The fusion of the modalities in a multimodal system is dependent on the architectural design which can be at the early, intermediate or the later stage of the process (Bubeck, 2003, Kisku et al., 2009).

- ## Voice Print and Teeth Pattern

Kim and Hong, (2008) use a multimodal of voice print and teeth image to authenticate a subject using the embedded camera in a mobile phone to capture the teeth. The proposal used a weighted-summation operation with 1000 teeth image and voice using 50 subjects. Each of the subjects had 20 teeth images and voice print for the experiment. The teeth image is detected by the dentition pattern on the teeth region using AdaBoost algorithm based on Haar-like features and the EHMM algorithm with 2DDCT as feature vector. The camera resolution used to capture the image is of 480 x 640 pixels that were normalized to 80 x 40 pixels after processing. The system uses Linear Discriminant Analysis (LDA) as sequential steps. Two-dimensional Discrete Cosines Transform (2D-DCT) and an Embedded Hidden Markov Model (EHMM) algorithm were used for the authentication phrase. For the voice, pitch and Mel-frequency Cepstral Coefficients (MFCC) was used as feature parameter while Gaussian Mixture Model (GMM) algorithm is used to model the voice signal. The training was done with 250 images and voice print with the remaining used for evaluation. In evaluating the performance, the average time for teeth pattern detection was put at 2.92s (55.97s for training) and 10.76s for authenticate. The EER for teeth authentication is 6.42% while voice is 6.24% with the two modalities put together achieving an EER of 2.13%. The issue with the use of the teeth for user authentication is that not everyone places the phone directly close to the mouth for easy capturing. The use of ear piece to receive and answer calls is also an issue in the authentication method because the teeth can't be captured for authentication.

- ## Voice and Face Multi-Modality

Using the same type of device for capturing the biometric data like Kim and Hong, Tresadern et al. (2013) fused voice print with face image for mobile phone authentication.

The system used the rough estimate of a position and size of the face to localize the captured image. The captured images are classified using modern pattern-recognition methods to learn the image characteristics which is then divided into 'face' or 'not face' image. The captured image is summarised as a facial region and uses a variant of the Local Binary Pattern (LBP) as the capturing algorithm. A facial future locator, Active Appearance Model (AAM) was developed with a fitting of a model of the facial parameter. The voice after capturing, like Kim and Hong (2008) used pitch and Mel-frequency Cepstral Coefficients (MFCC) as feature parameter while a Gaussian Mixture Model (GMM) is used to classify it as 'speech' or 'no speech'. The two modalities were classified independently before using score level fusion as a third classifier. The system EER performance is put at 9.69% for face and 2.29% for voice. Face user authentication issues have been highlighted in the last section. Speech on the other hand, is sensitive to a number of factors like noise at the background, emotion and physical state of the user, it is currently restricted to low-security because of its instability (Jain et al., 2000).

- ## Eyes and Face Multi-Modality

Boehm et al. (2013) presented a system known as SAFE (Secure Authentication with Face and Eye) to unlock a device. The SAFE system uses face to recognise the user while using the eye to trace a secret icon's path. The system uses a gaze-based challenge-response protocol using ITU Gaze Tracker (version 2.1). The system takes advantage of the gaze to capture the face. For error checking of the system, a methodical framework to implement the challenge-response protocol using Principal Component Analysis (PCA). A Canon Powershot SD1200IS digital camera is used to capture the face. The face is recorded while the user rotates his head slightly to the left and to the right with a face recognition online module in C/C++ using OpenCV for recognition. To extract the face features, Eigenface

and the geometry (triangle) between two eyes and the mouth were used. Using thirteen participants, eight pictorial images were taken during enrolment that is used for matching after images are captured from a video that streams continuously and matching each image taken for the face recognition system. The disadvantage of the method is that the user is actively involved in the process. That mean any time the phone is to be answer the user must gaze at the phone before a proper authentication is done. This will be inconvenience to the user, therefore have a usability issue.

3.3.3 Conclusion

In conclusion, the used of transparent authentication is to improve the use of biometric for user authentication. The discussed transparent authentication methods as listed in Table 3.2 used different identification method to achieve the aim of their work. They have their advantages and disadvantages depending on the method of extracting the biometric data. The different modalities discussed have issues in term of the methods used for extraction the data for authentication. For example, the use of mobile phones camera for authentication has an issue of accurately capturing the facial data if not consciously used to capture the targeted image; the same applies to teeth etc. Gait authentication can only be done when the subject is walking and most subject use the phone more when not in motion. Therefore, the improve on the biometric for easy implementation of transparent authentication, bioelectrical signals gives added advantage because it can be captured irrespective of the subject action, position or location.

Table 3.2: Current Transparent Authentication Systems Work and Performance

Table 1

Authors	Identification method	Classifier	Duration	Feature extracted	No of Sub.	Performance
(Frank et al., 2013)	Phone surface ion	*k*-nearest-neighbors (*k*NN) Support Vector Machine (SVM)	25-50 minutes	Touch screen interact	41	0% and 4%
(Campisi et al., 2009a)	Keystroke (keypad)	Statistical	3hrs and 6hrs	Keystrokes	62 & 40	EER of 13%
(Jayamaha et al., 2008)	Voice	Hidden Markov Model (HMM)	20ms and 40ms.	Voice Print		(86.25% success
(Kim and Hong, 2008)	Phone Camera	EHMM (Embedded HMM and Gaussian Mixture Model (GMM)	250 images and voice	Voice and Teeth print	50	EER of 2.13% and 2.8%
(Venkataramani et al., 2005)	Phone Camera	Correlation filters,Individual PCA, and FisherFaces		Facial image	20	EER of 1.1%.
(Tresadern et al., 2013)	Phone Camera	Gaussian Mixture Model (GMM)		Voice and Face image		EER: Face-9.69% Voice-2.29%.
(Tang et al., 2010)	Phone Orientation and GPS	Directional graphs and a rule-based classifier	15 days (10:data collection : 5 training)	Orientation sensor, data mining and GPS information	10	EER of 0.76%.
(Clarke and Mekala, 2007)	Word Signature			Use of common words	20	FAR and FRR of 0 and 1.2%
(Nickel et al., 2011)	Gait	SVM, The Mel-frequency Cepstral Coefficients (MFCC) and Bark Frequency Cepstral Coefficients (BFCC)	37 meters	accelerometer signals from tri-axial	48	NMR of 59.9% at a FMR of 1.3%

3.4 The Use of Bioelectrical Signal for Transparent Authentication

The discovery of Biological system electricity as a signal was first discussed by an Italian physicist Luigi Galvani in 1789 (Jeong, 2011). They are generated by different body activities which includes the Heart, the Brain, Muscle movement and others (Fabbri et al., 2010). They are the phenomenon of life in a body cell and is the smallest unit of life, it constitute the building block of every living creature (Charman, 1990, Tricoche et al., 2008). Work by Joseph (Pancrazio et al, 1998), discussed bioelectrical signal in his work, where excitable cells are recorded while Shingo in his work (Kawamoto et al, 2012) associated bioelectrical signals to Electrocardiogram (ECG) and Electroencephalogram

(EEG) which was used in his work too. Therefore, bioelectrical signal can therefore be defined as:

"*The electrical current generated by the internal body activities from a living cell*".

Bioelectrical signals are very low frequency signals that are mostly used for medical purpose. There are several bioelectrical signals which include Electrocardiogram (ECG), Electroencephalogram (EEG), Galvanic skin response (GSR), Skin Temperature, Electromyogram (EMG), Mechanomyogram (MMG) and Electrooculography (EOG). Some of the bioelectrical signals will be use in the thesis therefore will be defined.

- **Electrocardiogram (ECG):** ECG is the electrical recording of the rhythmic beat of heart. In analysing the frequency and pattern of the heart, information like the heart rate and heart rhythm can be extracted. ECG recording takes long timescale and can take up large data space (RNMO and Laguna, 2006). The dectection and comparison is based on the characteristic points (P, Q, R, S, T) in ECG waveform. ECG is divided into two phrase of depolarization and repolarization of the heart muscle fibers. The depolarization is made up of the P-wave (atrial deportation) and QPS–wave (ventricular depolarization) and the repolarization phases, the T-wave u-wave (ventricle repolarization) (Biel et al., 2001).
- **Electroencephalogram (EEG):** Electroencephalogram (EEG) is the measurement of the brain waves. There are four basic brain wave patterns that range from 0.5 to 100 microvolt in amplitude (Teplan, 2002). These wave pattern are beta (>13 Hz), alpha (8-13 Hz), theta (4-8 Hz), delta (0.5-4 Hz).
- **Galvanic skin response (GSR):** Galvanic skin response (GSR) is the measurement of change in the electrical property of the skin. This is the change of balance of positive

and negative ions which result to change in current flow within the skin. This can be recorded using two electrodes places on the skin. With the improvement of mobile device, some of them like smart watches use sensor to extract the GSR.

- **Skin Temperature:** The skin temperature is the temperature regulation between the internal and the surface body temperature. An average skin temperature ranges between a certain degree and can change depending on the health of the subject.

These bioelectrical signals are physiological modalities in which features that can be extracted (Pal et al., 2015). In processing bioelectrical signal for authentication, three main stages are followed to achieve the end product of user authentication system as illustrated Figure 3.4. These processes are pre-processing, feature extraction and classification /training (Tamil et al., 2008).

Figure 3. Error! No text of specified style in document.**.4: Block diagram for processing bioelectrical signal system for authentication.**

To employ bioelectrical signals for user authentication, the bioelectrical signals need to be investigated to know the best pre-processing, feature extraction and classification method to use. Therefore, some investigations and studies on the use of ECG bioelectrical signals for authentication are carried out for this thesis. ECG is used for the investigation the activities of the heart rate. Therefore, it will be necessary to study the feature extraction and classifiers used by various researches. Table 3.3 shows that different works used different methods for feature extraction and classification to achieve authentication.

Table 3.3: Feature Extractor and Classifier for bioelectrical signals.

Author/Year	Signal	Feature Extractor	Classification	Success rate
(Israel et al., 2005)	ECG	Morphological Features	linear Discriminant Analysis (LDA)	97-98%
(Shen, 2005)	ECG	Morphological Features	Quartile Discriminant Measurement (QDM)	100%
(Kim et al., 2006)	ECG	Q-wave, R-wave and S-wave (QRS) Detection	Mahalanobis Distance	-
(Subasi, 2007)	EEG	Wavelet Transform	Expectation–Maximization	94.5%
			Multi-layer Perceptron Neural Networks (MPNN)	93.2%
(Wang et al., 2008)	ECG	Detection, Morphological Features (QRS) and Principal Component Analysis (PCA)	K-nearest Neighbor and LDA	94.47% and 97.8%
(Gahi et al., 2008)	ECG	Morphological Features	Mahalanobis Distance	100%
(Cvetkovic et al., 2008)	EEG	Wavelet Transform	Support Vector Machine	-
(Chan et al., 2008)	ECG	Wavelet Transform	Correlation Coefficient	89% - 95%,
(Hema et al., 2008)	EEG	Welch Algorithm	Neural Network	94.4 to 97.5%
(Kousarrizi et al., 2009)	EEG	Ample Maximum & Sample Minimum,	Neural Network	68 – 100%
(He and Wang, 2009)	EEG	Independent Component Analysis (ICA)	Gaussian Mixture Models (GMM) and Maximum Posteriori Model Adaption (PMA)	5.0%
(Sasikala and Wahidauanu, 2010)	ECG	QRS Detection	Correlation Coefficient (CC)	99%
(Ye et al., 2010)	ECG	ICA and Wavelet Transform	Support Vector Machine	99.6%
(Coutinho et al., 2010)	ECG	Morphological Features	Lempel-Zil	100%
(Hema and Osman, 2010)	EEG	Power Spectral Density	Neural Network	78.6%.
(Tawfik and Kamal, 2011)	ECG	Discrete Cosine Transform	Neural Network	99.09%
(Sidek and Khalil, 2011b)	ECG	Wavelet Transform	Radian Basis Function	91%
	EEG	QRS Detection and Wavelet Transform	Radian Basis Function	95%
(Hema and Elakkiya, 2012)	ECG	Power Spectral Density (PSD)	Neural Network	97.2% to 98.85%
(Zokaee and Faez, 2012a)	ECG	Mel Frequency Cepstral Coefficients (MFCC)	KNN	89%
(Lee et al., 2012)	ECG	QRS detection	Support Vector Machine	85.04%
(Mohanchandra et al., 2013)	EEG	PSD	PCA	85 %

The feature extraction method should be good enough and should meet some properties like repeatability, distinctiveness, quantity, accuracy, and efficiency (Tuytelaars and Mikolajczyk, 2008). From the different research, Morphological Features, QRS Detection, Wavelet Transform, Independent Component Analysis and Power Spectral Density are among the most used feature extraction methods. Each of the methods do have advantages and disadvantages depending on the type of bioelectrical signal extracted. QRS Detection has the advantage of efficient extraction of beat-to-beat intervals (RR) from long Electrocardiogram (ECG) recordings with a disadvantage of implementation in software (Arzeno et al., 2008). Another disadvantage is that it cannot operate in real time and it is

also suitable for real-time analysis of large datasets (Stojanovic et al., 2011). Wavelet Transform has a varying window size, being broad at low frequencies and narrow at high frequencies, It is better suited for analysing of sudden and transient signal changes (Sidek and Khalil, 2011b), Better poised to analyse irregular data patterns, that is, impulses existing at different time instances (Al-Fahoum and Al-Fraihat, 2014). The classification methods such as Neural Network and SVM are the most used. Neural Network can perform better in nonlinear statistical modelling and is an alternative to logical regression (Tu, 1996). SVM performs better classification on emotional features which is prevalent in EEG signal (Riera et al., 2008).

3.4.1 Pre-processing of Bioelectrical Signal

In signal processing, the type of signals and their behaviours is considered while processing the signal. A non-stationary signal can be of different frequencies because it changes as a function of time (Hammond and White, 1996). They come with ransom components like random noise, spike and other factor affecting the quality of the signal (Moukadem et al., 2014). In this case the signal extracted from the wearable device might contain noise because of the wireless signals around which can affect the signal quality (Sidek and Khalil, 2011a; Hema and Elakkiya, 2012; Zokaee and Faez, 2012b). These noises need to be removed but the source of the noise is first identified to know the most appropriate method to be applied in removing the noise. Noises in a bioelectrical signal can be categorised into the following (Zokaee and Faez, 2012b):

- Power line interference
- Baseline wandering
- Electronic pop or contact noise
- User - electrode motion artifacts

Noise reduction in a signal is expected to improve the signal quality using a filter (Sidek and Khalil, 2011a). Therefore, the pre-processing will involve noise removal through filtering before the feature will be extracted. To remove or reduce the noise in the bioelectrical signal, the decomposition into sub-band using wavelet eliminates noise as part of the decomposition process. Research has shown Wavelet Transform process in the feature extraction has been used for de-noising signals (Lau, 2016, Chen and Bui, 2003).

3.4.2 Feature Extraction for Bioelectrical Signal

The feature extraction process plays a major role in the use of bioelectrical signal for authentication. The extracted features from bioelectrical signal has been proven to be unique enough for authenticating an individual (Nandish et al., 2012). From the different types of techniques discussed and after investigating the properties of the bioelectrical signals, the Wavelet Transform feature extraction technique is adopted. The use of Wavelet Transform is becoming popular in the measurement and analysis of time-frequency nonstationary signals and the spectral component variation (Mallat, 1989, Addison et al., 2009). The signals changes as a function of time therefore the extraction technique should be able to predict the signal pattern (Hammond and White, 1996). Wavelet transform is also useful in processing different types of transient signal analysis (Gokhale and Khanduja, 2010). Waveform transform for feature extraction can be implemented using different process depending on the type of bioelectrical signal to be processed. It decomposes a signal into sub-bands that can be implemented with several wavelet families. For the purpose of this work, Discreet Wavelet Transform (DWT) and Wavelet Packet Entropy (WPE) feature extraction methods are discussed and used for the feature extraction of the bioelectrical signals.

- **Discreet Wavelet Transform (DWT)**

DWT decomposition splits the input signal into Approximation Coefficients and Detail Coefficients as shown in Figure 3.5 (Bo-zhi and Hong-bin, 2008, Gokhale and Khanduja, 2010). The decomposition enables the signal to be analysed at the different *n* levels as shown in Figure 3.6 (Tsai, 2002).

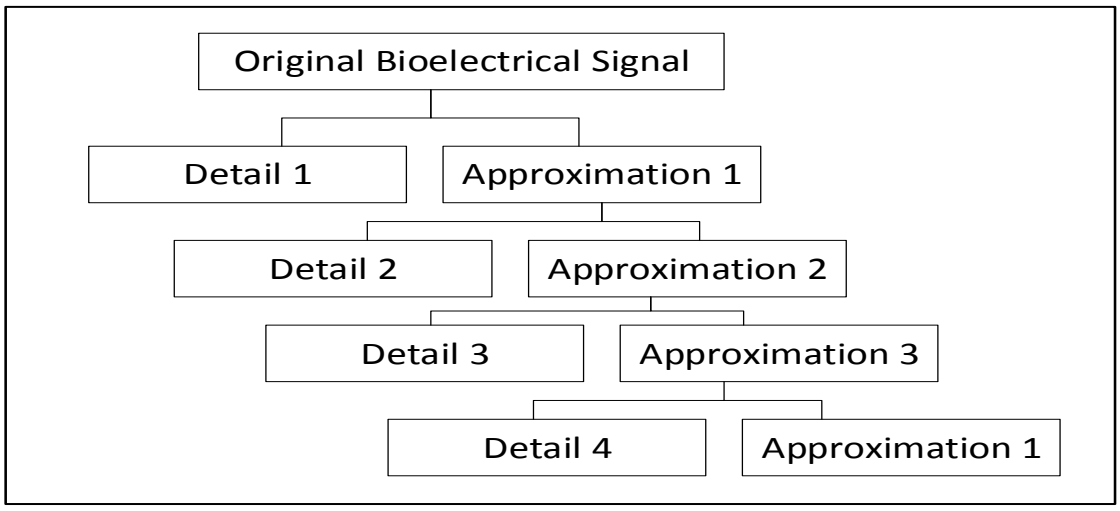


Figure 3. Error! No text of specified style in document..**5: Decomposition of approximation coefficients and detail coefficients**

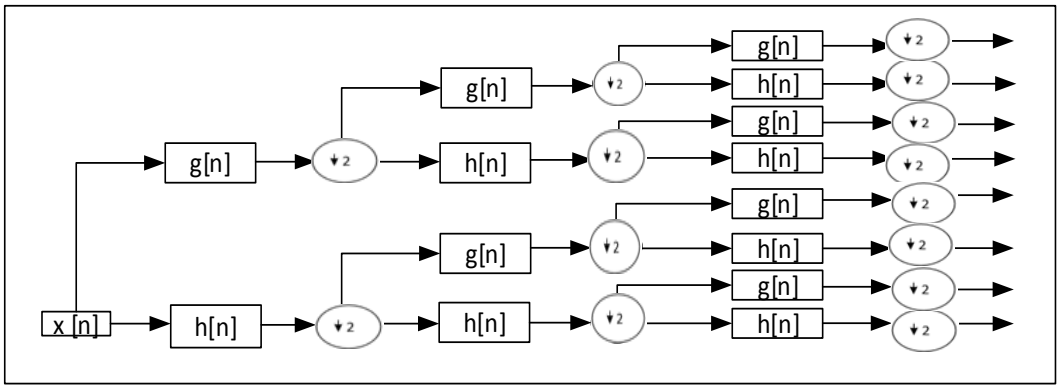


Figure 3. Error! No text of specified style in document..**6: Wavelet decomposition over 3 levels.**
g[n] is the low-pass approximation coefficients, h[n] is the high-pass detail coefficients

Each *n* level is further decomposed into a high and low frequency signal component using a filter bank (Gokhale and Khanduja, 2010, Laine and Fan, 1993). The decomposed sub-band *g(n)* is the low-pass approximation coefficients while the *h(n)* is the high-pass detail coefficients.

- **Wavelet Packet Entropy (WPE)**

Wavelet packet entropy feature extraction is chosen because it provides useful information for investigating non stationary signals just like discrete wavelet transform (Safara et al., 2013). Entropy provides useful information for classifying electrical power data, energy information etc. just like body temperature (Hu et al., 2008). Several studies have implemented an identification system applying entropy (Chen and Liginlal, 2008, Thiemert et al., 2006, Cachin, 1997, Bulusu and Plesniak, 2015).

3.4.3 Bioelectrical Signal Feature Selection

Optimal feature selection is relevant before its application for classification. It is an important factor for accurate discrimination of subjects because it influences the result output (Cvetkovic et al., 2008). Feature selection process is an active research area because the extracted features represented the most informative content in the dataset. Some of the

information in a signal for pattern recognition techniques are irrelevant therefore the need to carefully select the feature vectors that is important and useful. Also feature selection also minimizes the computational cost and time to process the classification by only using useful features. This is done by using different evaluation criteria that best represent a pattern for identification (Dickhaus and Heinrich, 1996).

3.4.4 Classification of Bioelectrical Signal

Neural network is one of the most widely used classifier in bioelectrical signal classification. Neural network used as classifier by different researcher includes (Subasi, 2007, Hema et al., 2008, Kousarrizi et al., 2009, Tawfik and Kamal, 2011, Hema and Osman, 2010). Other classifiers used includes Correlation Coefficient (CC) (Chan et al., 2008); Linear Discriminant Analysis (LDA) (Shen, 2005); Support Vector Machine (SVM) (Cvetkovic et al., 2008, Ye et al., 2010); Mahalanobis Distance (Kim et al., 2006, Gahi et al., 2008); Radial Basis Function (RBF) (Sidek and Khalil, 2011b); Multi-layer Perceptron Neural Networks (MLPNNs) (Subasi, 2007).

3.4.5 Context Awareness in User Authentication

The ubiquities of smart mobile phones have enhanced the extraction of variety of information which includes but not limited to the phone user location. This could be used to predict a user geographical location at any point in the day. There has been research in understanding context and its development for the context aware application (Abowd et al., 1999). Some of the research includes context aware computing for monitoring the environmental change (Covington et al., 2002). Another use of context awareness is for security purpose, Michael in his work used context awareness application for security challenges in the home (Covington et al., 2001). Therefore, the application of contextual data is used in enriches the information provided for security. The used of context

awareness for user authentication will improve the available information for discrimination of user in mobile security.

3.5 Discussion

A number research groups, companies has put forth proposers or developed some gargets or wearable technologies to meet the different demand for biometric authentication/verification in the development of future security system (Gafurov, 2010). There has been research and investigation on the use of bioelectrical signal generated from the heart, brain etc. for authentication (Biel et al., 2001, Chatra, 2014). Phyode introduced W/ME wristband with EKG sensor to detect bioelectrical activity like the heart rate (Technologies, 2013). In another development, Apple released a smart watch with the capacity to extracted bioelectrical signals from the body and transmits it to its Apple IPhones. With many more wearable coming on board, their usage for further applications will also be explored to gain maximum benefit that comes with these new technologies. To meet the present user authentication need, a user authentication on mobile device can get better if the authentication process is done without the active participation of the user before the process is done. The authentication should be transparent to the user, a process without the knowledge of the user. It should be able to re-authenticate the user within a short time frame interval that will make the system continuous.

3.6 Conclusion

There has been several works on transparent user authentication using biometric modalities. Most of the works focus on authentication at the point of entry while some goes further to re-authenticate a subject after the initial authnetication. This improve the

authnetication process however the authentication process is still intrusive which leads to inconvenince on the part of the subject. The issues of usability should be considered along side security like in the case of Iphone 6 where the home button is used to transparently authenticate the user, the process is transparent but still intrusive at the point of entry to continously authneticate the user. Within transparent authentication, there are wealth of literature looking at modalities and techqnics to improve the process of transparent authentication using emerging modalities.

This chapter has discussed different modalities deployed to improve transparent authentication with several facing one issue or the other in term of usability. To overcome the issue of usability while not conpromising the security of a user authentication system, this next chapter will introduce the use of bioelectrical signals for implimenting a transparent user authentication that will take into account security as well as usability.

4. Bioelectrical Signal Evaluation and Feature Extraction

4.1 Introduction

In a user authentication system, there are different processes involved from the data extraction to the actual authentication of the subject. The procedures follow a set of standard methodology that includes data collection, feature extraction, classification etc. for successful authentication of a subject. This chapter first of all presents the bioelectrical signal data collection procedure. In the process of extracting the data, some fundamental issues are identified and solution proffer for a successful data collection. Feature extraction plays an important role in a user authentication process therefore feature selection is employed to choose the most suitable features to extract from the bioelectrical signals for classification. The research presented a preliminary experiment as a prelude to the major experiments. The expectation of this research is to develop a transparent and non-intrusive user authentication system. To achieve this, the following research question will be answered in this chapter:

1. What exiting wearable device can be used for acquiring bioelectrical signals and context awareness data for implementing a transparent biometric user authentication?
2. How will the bioelectrical signals be extracted through a non-intrusive method to overcome the issue of inconvenience as mentioned in the literature review?
3. How viable are the bioelectrical signals extracted from the wearable device for user authentication?
4. The suitability of the extracted features to successfully discriminate subjects to achieve an acceptable identification rate

4.2 Technology Evaluation and Data Extraction

Most wearable technology manufacturers today have incorporated various sensors to get better market share over their competitors. To achieve a transparent and non-intrusive method for user authentication, this section seeks to answer the first research question on employing any exiting wearable technology that can achieve the aim of the research. The research chooses four wearable technologies suitable for acquiring the biometric data needed. The wearable device selected includes Mio Fuse, Fitbit charge HR and The Microsoft Band which are all smart watches. A fourth waerable, Polar H7 Heart Rate monitor is a chest strap for monitoring the heart rate. The Polar H7 is use as the base device for measuring the accuracy of the three smart watches. The different smart watches can extract and save their extracted data on a mobile device using their various proprietary applications. The data extracted from all the watches are saved on the same smart phone for evaluation.

4.2.1 Wearable Devices

- **Polar H& heart Rate Monitor**

Polar H7 Heart Rate monitor is a light weight adjustable chest strap with a heart rate monitor using a Bluetooth transmitter to communicate with a mobile device. The monitor can only monitor heart rate. The chest strap heart rate monitors are more accurate than other wearable device worn on any other part of the body for heart rate monitoring because they are more intrusive (Zhan, 2012). The heart rate monitoring can be transmitted to a mobile device and store on it through Bluetooth connection.

Figure 4. 1: Polar H7 heart beat Monitor

- **Mio Fuse**

This wearable technology is a sleek wristband with features like heart rate monitor and other activity tracking capability. The heart rate monitoring is done from the wrist without requiring chest strap. The Mio Fuse arm band can be connected through Bluetooth to a mobile device with the help of a mobile application. The official app for Mio Fuse is called '*Mio Go'*. It has an advantage of setting the band features from a mobile device. There are other third-party applications like Strava, Wahoo, MapMyRun, MapMyRide, Endomondo, and more that can also be used with the Mio Fuse. When recording, the device can be set to indicate the user arm the watch is worn. The band uses an electro-optical cell to sense the volume of blood under the skin with an algorithms applied so that the heart's true rhythm can be detected. The Mio Fuse has some advantages which include easy synchronization between the band and a mobile device. It can be customized to exclude some feature not needed. The heart rate recording is a continuous one and is in beat per minutes (BPM). There are some disadvantages which includes draining of the battery which runs down fast if heart rate recording is done all day.

Mio Fuse heart rate monitoring is done in seconds, every second it picks up the heartbeat with the heart rate beats divided into zones. The zone is from 1-5 with a beat range which can be set to each zone with a time spend on each zone during recording. It also states the recording time in hour, minute and second as *"exerciseHour", "exerciseMinute", and*

"exerciseSecond", the length of recording and the date of recording. It also stores other data like average speed, best time, and average pace and estimate calorie burned.

Figure 4. 2: Mio Fuse

- **Fitbit Charge HR**

The Fitbit Charge HR is a smart watch activity tracker with many capabilities including daily steps, calories burned by day, monitoring sleep by night and a continuous heart rate monitoring. The heart rate monitoring is tracked with optical sensor which can be done in two ways of a continuous 24/7 heart rate monitoring or a work out monitoring. The Fibit can monitor the heart beat and store the data without a mobile device. This can later be transmitted through a hardware Bluetooth device to a personal computer/device; the information is stored in the cloud. The data can be access from a dashboard after an account has been opened on Fibit website. Fitbit provides a web API for accessing data. To develop an application to interact with the Fitbit Charge HR, a Fitbit Developer account is created to access it through the dashboard.

Figure 4. 3: Fitbit Charge HR

- **The Microsoft Band**

The Microsoft band is a 1.4 inch full colour touch screen hand band with many sensors built into it. It provides hourly or daily summaries of the activities recorded which includes calories, heart rate, distance covered, etc. The Microsoft band sensors can be access through software development kit (SDK) by a third party developer which is an advantage over others. It also has a Microsoft Health Cloud application programming interface (API). It is compatible with Android, Windows and iOS devices. Just like Mio Fuse the heart rate recording is also a Continuous one in beat per minutes (BPM). The band supports Android 4.3, Windows 8.1, iOS 7.1and above. The Microsoft Band recorded data can only be collected from the Microsoft dashboard from the online account. The data can be exported as CSV or Excel file format. The data stored includes the heart rate peak, heart rate low peak, the start and end time of the activity, average heart rate calories burned etc.

Figure 4. 4: Microsoft Band

4.2.2 Wearable Device Accuracy

To answer the first research questions, The three smart watches were evaluated with the aim of selecting the most suitable for extracting the biometric data for the user authentication system implimentation. To do this, an expereiment is executed to compare the three smart watches. The experiment will evaluate the three bioelectrical signals acquired from the three wearable device worn on the wrist and compare it against the one worn on the chest. The heartrate signals are generated from the heartbeat that is located within the chest part of the body. Therefore, it is not out of place to use wearable device worn on the chest as the reference device for accuracy evaluation. To appraise the accuracy of signals extracted from the wearable devices, the extracted heart rate signal from the devices are compared again the region which is most accurate proven point for measuring heart beat rate (Reiss and Stricker, 2012) as illustrated in Figure 4.5.

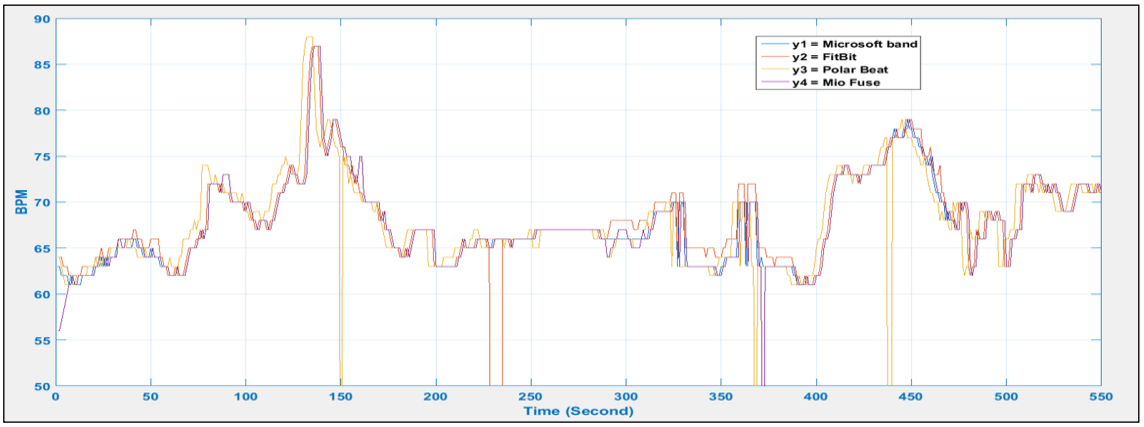


Figure 4. 5: Bioelectrical recording from the Microsoft Band, Fitbit, Polar HR & Mio Fuse

It is observed that not all the wearable started the extraction at the beginning of the data extraction. Polar HR and Fitbit started on the fourth second of the 550-second extraction; the Microsoft band started on the third second; while the Mio Fuse did not extract the data till after about 8 seconds into the extraction. From the graph, it observed that Polar HR and the others have some level of difference; this is because the Polar HR is more intrusive

than the others are. The three wearable devices of Fitbit, Mio Fuse and the Band worn on the wrist are almost accurate with the Polar Beat worn on the chest with slight difference noticed mostly in Fitbit and Mio Fuse. The three-wearable device have some millisecond level of accuracy there the differences is not noticeable and make no difference.

4.2.3 Wearable Capacity Evaluation

The Fitbit, Mio Fuse and the Microsoft Band evaluation are also based on the number of sensors and other information that can be extracted to support the bioelectrical signals to be extracted. The Mio Fuse has some advantages, which include easy synchronisation between it and the mobile phone but with few sensors compared to other. The Fitbit Charge HR is a smart watch activity tracker with many capabilities including daily steps, calories burned by day, monitoring sleep by night and a continuous heart rate monitoring. The Microsoft Band extracted data can only be collected from the Microsoft dashboard from the online account but allows a third application to extract the data. This give advantage to its use. The Microsoft Band uses an electro-optical cell to sense the volume of blood under the skin. The data can be exported as CSV or Excel file format. The data stored includes the heart rate peak, heart rate low peak, the start and end time of the activity, average heart rate calories burned etc. Table 4.1 shows more information about the four wearable devices.

Table 4. 1**: Wearable Technologies Requirement and Measurement**

	DATA INFORMATION	FITBIT CHARGE HR	MICROSOFT BAND	MIO FUSE	POLAR H7 HR
DATA	BEAT RATE	BPM	BPM	BPM	BPM
	STAIRS CLIMED	YES	YES	YES	NO
	DISTANCE WALKED	YES	NO	NO	NO
	CALORIES BURNED	YES	YES	YES	No
	SLEEP METRICS	YES	YES	YES	No
	STEP COUNTED	YES	YES	NO	No
	MESUREMENT TYPE	OPTICAL	OPTICAL	OPTICAL	ECG
	DATA EXPORT	YES (PAID OPTION)	YES	YES	YES
SENSOR	Heart Rate	Yes	Yes	Yes	Yes
	Global Positional System	Yes	Yes	No	No
	Accelerometer/Gyroscope	Yes	Yes	No	No
	Ambient Light Sensor	Yes	Yes	No	No
	UV Sensor	Yes	Yes	No	No
	Altimeter	Yes	No	No	No

	Galvanic Skin Response	Yes	No	No	No
	Skin Temperature	No	Yes	No	No
FUNCTION/	Body Placement	Wrist	Wrist	Wrist	Chest
	Data Transfer	Bluetooth Smart	Bluetooth Smart	Bluetooth Smart	Bluetooth Smart
	GSP Build-in	No	Yes	No	No
	Battery Life	5 Days	2 Days	14 Days	1 Year
	Battery Type	Researchable	Researchable	Researchable	Coin Cell CR2032
SOFTWARE	Web Application	Yes	Yes	Yes	Yes
	PC Application	Yes	Yes	Yes	No
	MAC Application	Yes	Yes	Yes	No
	Phone Application	IOS/Android/windows	IOS/Android/windows	IOS/Android	IOS/Android

After a critical look and the data information available from the three-wearable device of the Fitbit, Mio Fuse and the Microsoft Band, The Microsoft band is chosen because of its ability to extract more bioelectrical signals and contextual information data compare to others. Therefore, the smart watch of Microsoft band 2 that is a higher version of the Microsoft band will be used for data acquisition in this research.

4.2.4 Dataset Extraction Methodology

Most biometric authentication systems are faced with stringent condition when a biometric sample is to be acquired. Most of the data samples from the previous experiments are control samples (Israel et al., 2005, Kim et al., 2006, Sasikala and Wahidabanu, 2010). While this is ideal in some experimental studies, a typically highly controlled lab environment fails to understand the variance that would be exhibited from a real-life data capture. To this end, this work used a real-life data for the experiment and to answer the second research question. The selected smart watch is configured to extract the required data transparently and non-intrusively. To extract the bioelectrical signal, the Microsoft band2 is used to extract or acquire the data and transferred and stored on a smart phone. The Microsoft band2 and the smart phone communicate via Bluetooth connection to extract the data using four third-party applications installed on the smart phone. These applications are *Auto connect Bluetooth device, the Companion for Microsoft Band, AutotsaY* and *the Microsoft health.*

The goal in this research is to use a dataset that captures the natural activity of each user and to do so transparently. The second question, the method of acquiring the biometric data in a non-intrusive manner for user authentication will answered in this section. In this chapter, several experiments are used to achieve the aim. This is made possible by the installation of applications to extract the bioelectrical signals and contextual data. The process of the data extraction includes the combination of different third-party applications with the device application are installed on the phone to successfully extract the biometric data. Four applications are integration to do different function within the mobile device. The first application, the *Auto connect Bluetooth device* search for the Microsoft band2 through blue tooth, after discovery it establish a connection, locks it to the mobile phone. This is also done whenever there is disconnection between the Microsoft band and the mobile phone. This is important because whenever the user goes outside of the communication distance of the mobile phone, the mobile phone should re-establish communication with the Microsoft band when it comes within the communication distance between the two devices. After the connection of the two devices, the second application, *the Companion for Microsoft Band* (Processor, 2017) which is integrated with the Microsoft band2 propriety application *the Microsoft health* (Microsoft, 2018) starts to extract the data. The companion for Microsoft band application extracts the data and tabulated the information extracted to a file on the mobile phone as illustrated in Figure 4.4. The fourth application *Autostart and StaY* restarts *the Companion for Microsoft band* whenever it stops. The applications are integrated to overcome intrusiveness when the data are collected for the implementation of the authentication process.

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	DateTime	X	Y	Z	Stepping Gain	Steps Ascended	Steps Desc	Calories Toda	Status	Motion Typ	Pace	Speed	Resistance	X m/sÂ²	Heart Rate	Quality	Steps Toda	Total Steps	RR Interval
2	14/05/2017 11:22	-1.105225	-0.254639	0.036377	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-1.103516	72	LOCKED	2112	101074	0.713456
3	14/05/2017 11:22	-0.826172	-0.384033	0.12793	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-0.786865	72	LOCKED	2112	101074	0.713456
4	14/05/2017 11:22	-0.942627	-0.264404	0.278076	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-0.908691	72	LOCKED	2112	101074	0.680272
5	14/05/2017 11:22	-1.024414	-0.318359	0.282715	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-0.998535	72	LOCKED	2112	101074	0.680272
6	14/05/2017 11:22	-1.230713	-0.407227	0.221436	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-1.412354	72	LOCKED	2112	101074	0.680272
7	14/05/2017 11:22	-1.208496	-0.316162	-0.007813	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-1.057861	72	LOCKED	2112	101074	0.680272
8	14/05/2017 11:22	-0.855957	-0.281738	-0.197266	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-0.898926	72	LOCKED	2112	101074	0.680272
9	14/05/2017 11:22	-0.835938	-0.395752	-0.109375	109891	38310	37222	1222	WORN	WALKING	3125	32	340330	-0.845703	72	LOCKED	2112	101074	0.514352
10	14/05/2017 11:22	-1.093994	-0.341553	0.14209	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-1.067383	72	LOCKED	2114	101076	0.514352
11	14/05/2017 11:22	-1.054443	-0.501221	0.389893	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-1.173584	72	LOCKED	2114	101076	0.514352
12	14/05/2017 11:22	-0.984619	-0.512451	0.264893	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-1.090088	72	LOCKED	2114	101076	0.514352
13	14/05/2017 11:22	-0.560547	-0.647705	0.322266	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-0.594971	72	LOCKED	2114	101076	0.514352
14	14/05/2017 11:22	-0.553467	-0.723389	0.338135	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-0.574951	72	LOCKED	2114	101076	0.514352
15	14/05/2017 11:22	-0.385986	-0.813477	0.249756	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-0.413818	72	LOCKED	2114	101076	0.514352
16	14/05/2017 11:23	-0.521484	-0.782471	0.332764	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-0.462891	72	LOCKED	2114	101076	0.514352
17	14/05/2017 11:23	-0.435059	-0.694336	0.294678	109891	38310	37222	1222	WORN	WALKING	1818	55	340330	-0.522705	72	LOCKED	2114	101076	0.514352
18	14/05/2017 11:23	-0.572266	-0.814209	0.299072	109891	38310	37222	1222	WORN	WALKING	1470	68	340330	-0.567627	72	LOCKED	2114	101076	0.514352
19	14/05/2017 11:23	-0.512207	-0.833008	0.177246	109891	38310	37222	1222	WORN	WALKING	1470	68	340330	-0.508545	72	LOCKED	2114	101076	0.514352

Figure 4. 6: Data file extracted using Microsoft band

In the process of extracting the data, there are some issues faced. As expected in a real-life scenario, the possibility of environmental interference like noise (i.e. wireless and other Bluetooth connection) is expected. Before the dataset is extracted, an ethical approval for the data collection is applied for and approved in line with the University of Plymouth requirement. The dataset for this chapter is extracted at two instances. The experiment extracted all the four bioelectrical signals but used the heart rate extracted from 12 subjects for duration of 120 seconds and the second dataset heart rate signal extracted from 30 subjects for 360 seconds.

4.2.5 Evaluation of the Extracted Signal Variability

To answer the third research question, an activity-based experiment is used to examine the variability in the underlying bioelectrical signal. The evaluation of the extracted signal viability used the bioelectrical signal of the heart rate from five subjects out of the twelve subjects. The whole 120 seconds of the bioelectrical signal is used for the experiment. For this dataset, the experiment is controlled with activities like sitting, walking on a plain floor, walking down and up the stair case as illustrated in Figure 4.7

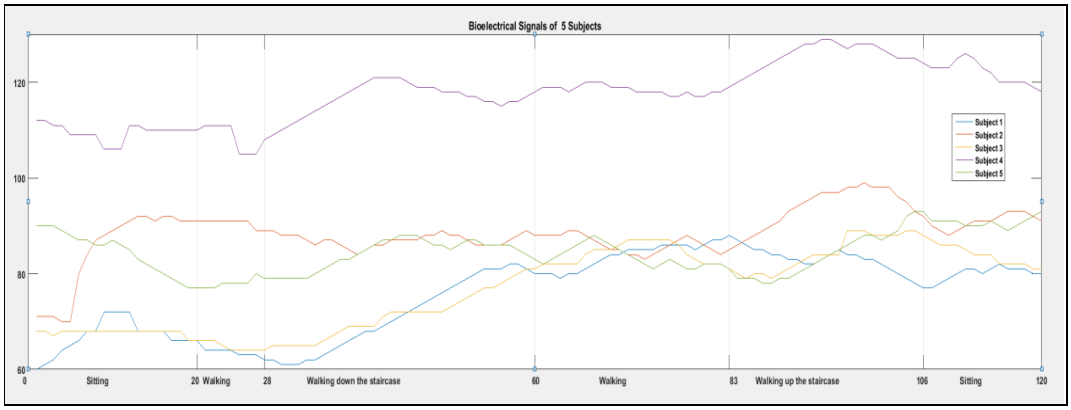


Figure 4. 7: Bioelectrical signal of 5 subjects showing the pattern variance among the subject.

The result of the variability of subjects as illustrated in Figure 4.3 shows that the five subjects are clearly differentiated. This shows potential for its use for user authentication. There are changes depending on the activity carried out by the subjects. This shows that different activities affect the heart rate pattern therefore this could be said of other bioelectrical signal to be extracted because of the similarity of their properties. The sitting section at the starting and end of the activities shows the signals are different though the same activity. This might be due to the heart beat less active at the beginning while the sitting at the end, the heart rate was very active before the sitting therefore, the heart rate is recovering from the active state. The walking section pattern is slightly different from the sitting but from the beginning of the walking down the staircase, the heart rate gradually increased across all the subjects. It stabilised slightly within a range at the walking section and at the walking down the staircase the heartrate increased again. Figure 4.8 to 4.10 shows three subjects doing the same activity three times and plotted to see the consistency in the signal pattern of subjects.

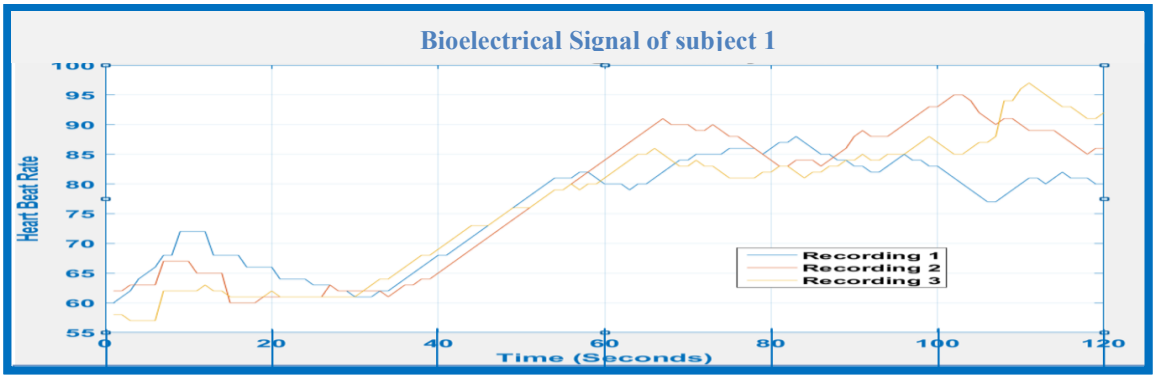


Figure 4. 8: Bioelectrical signal of subjects 1 showing three recording.

To further analysis the bioelectrical signals at this stage of this research, Signals from three subjects (Subject 1, 3 & 5) will be investigate to find the signals acquired from a subject has the same pattern. The data acquisition of the three subjects are done while carrying out a similar activity, the acquisition is carried for three different times which is compared against each other. The result shows similarity within the signals of each subject even though the subjects carried out the exercise at different times. The benefit of this experiment is to understand the effect of different activities on the heart rate bioelectrical signals.

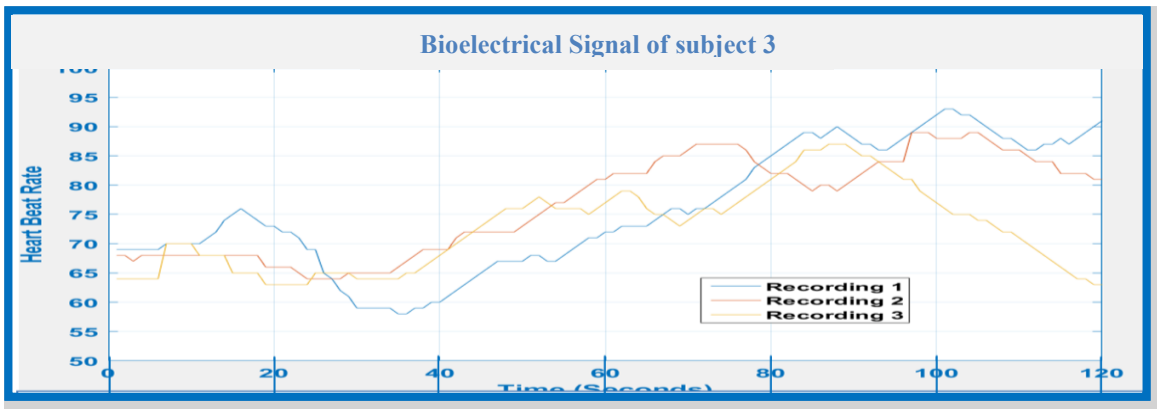


Figure 4. 9: Bioelectrical signal of subjects 3 showing three recording.

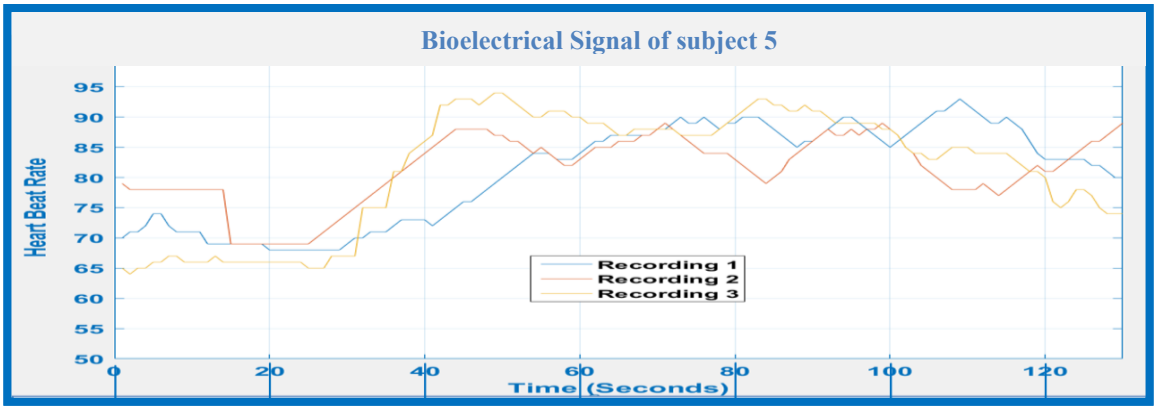


Figure 4. 10: Bioelectrical signal of subjects 5 showing three recording.

4.3 Experiment on the Features Selection

The technology evaluation has set the foundation for the research experiment to determine the feasibility of the used of bioelectrical signal extracted for user authentication. To determine the most suitable sets of features extracted for the rest of the experiments, a feature selection process is proposed. Statistical features are extracted from the heart rate signal while entropy features are extracted from the skin temperature and galvanic skin response using Discrete Wavelet Transform (DWT) and Wavelet Packet Entropy (WPE) feature extraction techniques respectively. To answer the fourth research question, an underlying methodology is used to investigate the best sub-set of features to apply on extracted data given a variety of tasks (e.g. walking, sitting) engaged in during the data extraction duration. The next section describes the feature extraction technique of DWT and WPE used for the feature extraction.

- **Feature Extraction Algorithm**

The feature extraction algorithm converts bioelectrical signal information into sets of feature vectors. However, the extraction technique will need to be carefully considered taking note of the non-stationary nature of bioelectrical signals. To apply bioelectrical signal for user authentication, it must meet the basic requirement and characteristics

needed to create a pattern for user authentication. Therefore it is expected that the signals should meet some characteristics like repeatability, distinctiveness, quantity, accuracy, and efficiency (Tuytelaars and Mikolajczyk, 2008). The wavelets transform techniques of discrete wavelet transform and Wavelet Packet Entropy features proposed for use are described. The fourteen statistical features extracted using discrete wavelet transform are listed as:

1. **Mean or Median absolute deviation:** these are the values diversity of the data around the median.
2. **Variance:** This is the sum of square distance of the bioelectrical signal.
3. **Maximum Amplitude**: This is the highest value in amplitude of the bioelectrical signal.
4. **Minimum Amplitude**: This is the lowest value in amplitude of the bioelectrical signal.
5. **Maximum Energy:** This is the highest value of the bioelectrical signal.
6. **Minimum Energy:** This is the lowest value of the bioelectrical signal.
7. **Mean of the energy:** This is the energy average value of the signal.
8. **Average Frequency:** This is the number of occurrences of a repeating event per unit time in the signal.
9. **Maximum Frequency:** This is the lowest point of the occurrences of a repeating event per unit time in the signal.
10. **Minimum Frequency:** This is the highest point of the occurrences of a repeating event per unit time in the signal.
11. **Standard Deviation:** This is the square root of the variance of a random variation.
12. **Peak2peak:** This is the difference between the maximum and minimum values of the bioelectrical signal.

13. **Root mean square level (RMS):** This is the value of a continuous-time waveform using square root of the arithmetic mean for calculation.
14. **Peak magnitude to RMS ratio:** This is the ratio of the largest absolute value in signal to the root-mean-square (RMS) value of the signal.

The wavelet Packet entropy features are Shannon entropy, energy entropy, threshold entropy, sure entropy, normalised entropy and power entropy.

1. **Shannon entropy:** measures the information content of a signal and its uncertainty (Fuhrman et al., 2000, Zhiwei and Minfen, 2007).
2. **Energy entropy:** this is the log energy of the signal. Energy entropy = wentropy (signal, 'log energy').
3. **Threshold entropy:** Compute threshold equal to 0.5 entropy of signal. Threshold entropy = wentropy (signal, 'threshold', 0.5).
4. **Sure entropy:** The Sure entropy measures the coefficient of a signal irrespective of the size simultaneously using threshold of 3 (Parak and Korhonen, 2014). Sure entropy = wentropy (signal,'sure', 3).
5. **Normalized entropy:** Compute norm entropy of the signal with power equal to 1.1. Normalised entropy = wentropy (signal, 'norm', 1.1).
6. **Power entropy:** Compute power entropy as Power entropy = (norm (signal) ^2)/length (signal).

- **Dataset for Feature Selection**

To study the discrepancy from one subject to another using the features available, the fourteen statistical and the six entropy features are evaluated depending on the bioelectrical signal to be use. DWT feature extraction technique is used for extracting the heart rate only for this experiment. The evaluation used the fourteen statistical features for

the Heart Rate (HR) signal while six entropy features are used for the Galvanic Skin Response (GSR) and Skin Temperature (ST) signals as illustrated in Table 4.2. As stated earlier DWT decomposes the signal into sub-bands, the first level detail coefficient of the sub-band is used to extraction the features for 12 subjects. The six entropy features are extracted from 5 subjects. The basis for using few numbers of features is predicated on the fact that mobile device power requirement is limited in capacity compared to personal computers (Carroll and Heiser, 2010). The features are extracting from 28 to 60 seconds of the 120 seconds signal section when the subjects are walking down the staircase.

Table 4. 2: Data information for feature selection

Bioelectrical signal	Number of subject used	Feature extraction technique	Number of features extracted
Heart Rate	12	Discrete Wavelet Transform	14
Skin Temperature	5	Wavelet Packet Entropy	6
Galvanic Skin Response	5	Wavelet Packet Entropy	6

4.3.1 Heart Rate Signal Features Selection

The feature variations are important in choosing the most effective features for classification of users. Fourteen statistical features are extracted from the 12 subjects. The features are computed with MATLAB using the first level detail coefficient of biorthogonal wavelet transform sub-band. The output was tabulated to show the variations as illustrated in Figure 4.11- 4.14. The feature selection plotting is divided based on the various feature scoring values. The x axis shows the different features scores while the Y axis show the scores. The disparity of score between the subjects and within the subjects shows good discriminatory information in the features. For example Figure 4.11 shows subject 11 and12 having different score of variance mean of energy and mean and for each

subject their feature scores are also different too. This is important as it is used to differentiate the subjects because of the different information provided by the features associated with each subject.

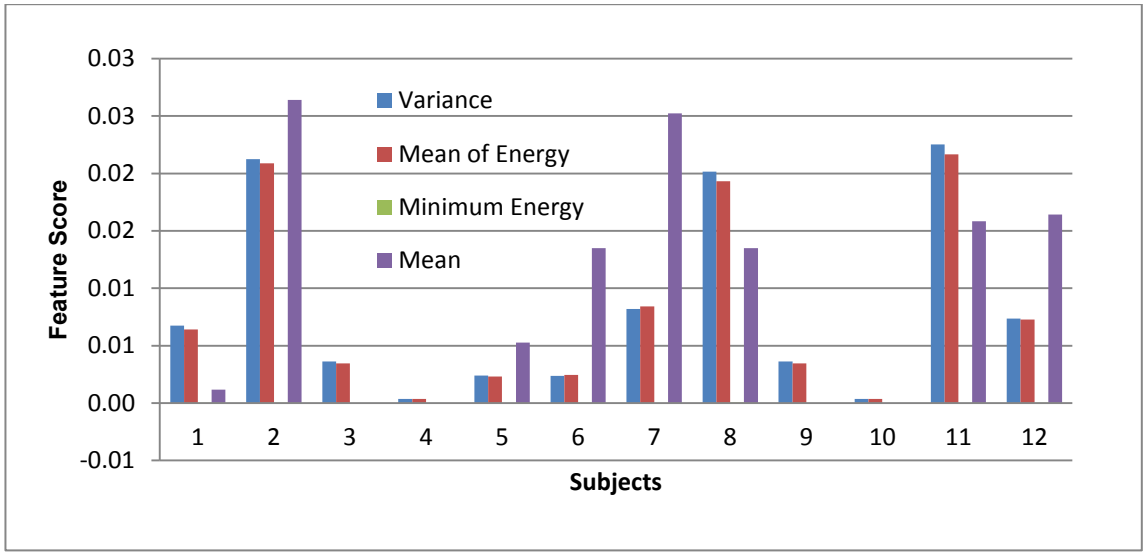


Figure 4. 11: Variation of Variance, Mean of the energy, Minimum Energy and mean on twelve subjects

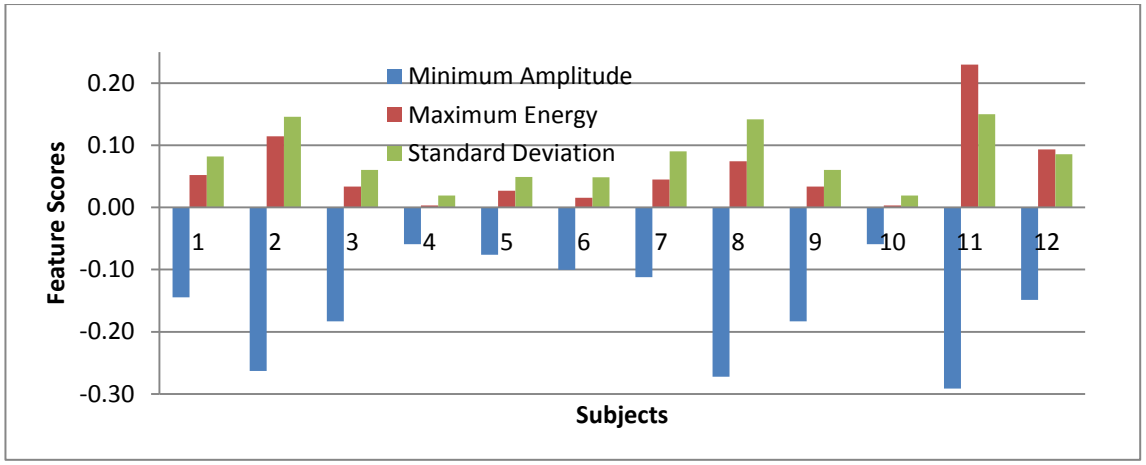


Figure 4. 12: Variation of Minimum Amplitude, Maximum energy, and Deviation on twelve subjects

Figure 4.11 values ranges from 0.0 to 0.03 with the mean having the highest value. The graphical representation shows that the variation of Variance and Mean of the energy

provides good value to discriminate subjects with Minimum Energy not having any value. The mean has value for some but not all the subjects. Therefore, the Minimum Energy and the mean will not be ideal for use to classify the subjects. The variation of subjects by the Minimum Amplitude, Maximum energy, and Deviation as illustrated in Figure 4.12 with values ranging from -0.29 to 0.23 provides useful discriminatory information, therefore the three will be selected for further feature extraction.

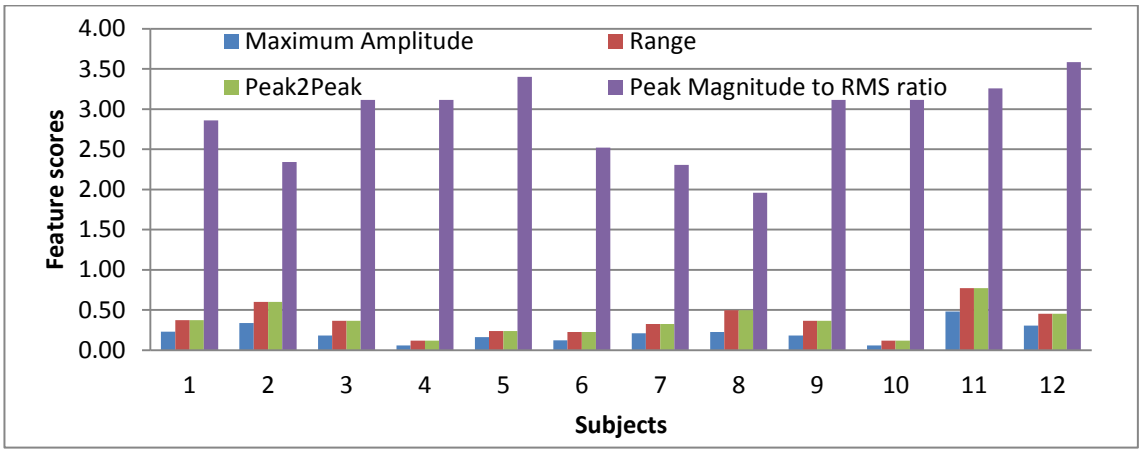


Figure 4. 13: Variation of Maximum Amplitude, Range, Peak2peak and Peak Magnitude on twelve subjects

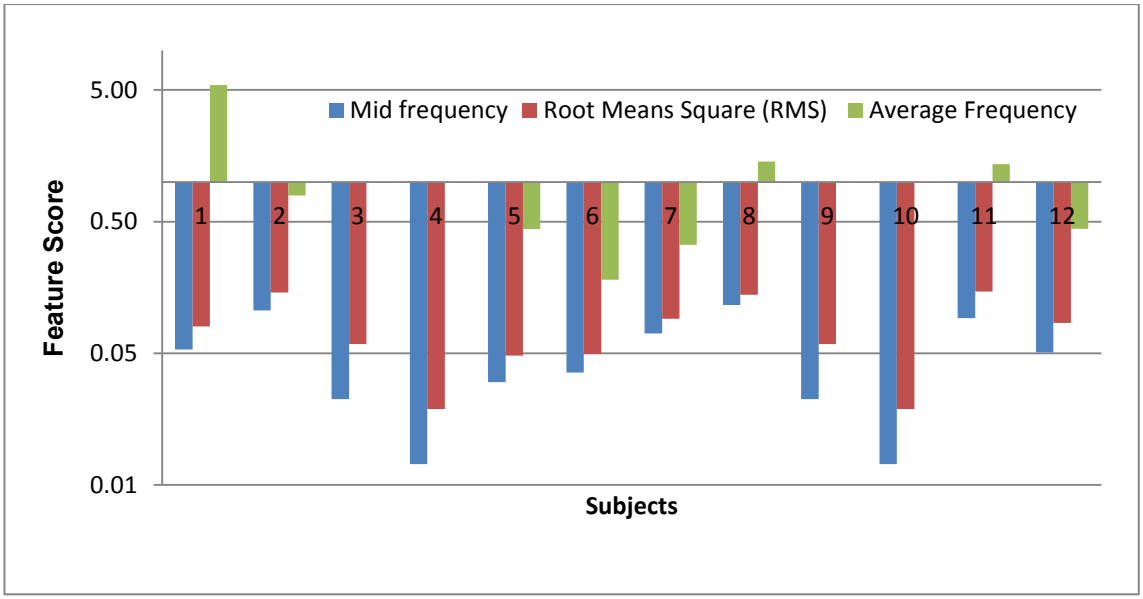


Figure 4. 14: Variation of Mid frequency, Root Mean Square and Average frequency on twelve subjects

Figure 4.13 showing the plot for variation of Maximum Amplitude, Range, Peak2peak and Peak Magnitude puts the Range and Peak2peak scoring the same value across all the subjects while the rest of the features shows good discrimination between subjects. All the features are selected except the Range and Peak2peak which have the same scores. Therefore one (range) is chosen as the use of the two features will not add value to the process since they represent the same value. There are variations in all the features in Figure 4.10 except the Average frequency. The Mid frequency and Root Mean Square will be selected while the Average frequency will be rejected for further feature extraction process. From the fourteen features, the variance, minimum amplitude, maximum energy, standard deviation, maximum amplitude, peak2peak, peak magnitude to RMS ratio, average frequency, root mean square (RMS) and peak magnitude were chosen.

4.3.2 Skin Temperature and Galvanic Skin Temperature Signal Feature Selection

To evaluate the Galvanic Skin Response and Skin Temperature bioelectrical signal, six entropy features are extracted from the galvanic Skin Response and Skin Temperature bioelectrical signals. Comparing the graphical results, it shows that the features extracted using discreet wavelets transform were not discriminatory enough to differentiate subjects for both the GSR and skin temperature as illustrated in Figure 4.15 and 4.16. The statistical features from the GSR have shown only one feature was able to discriminate the subjects while the other has insignificant output across all subjects.

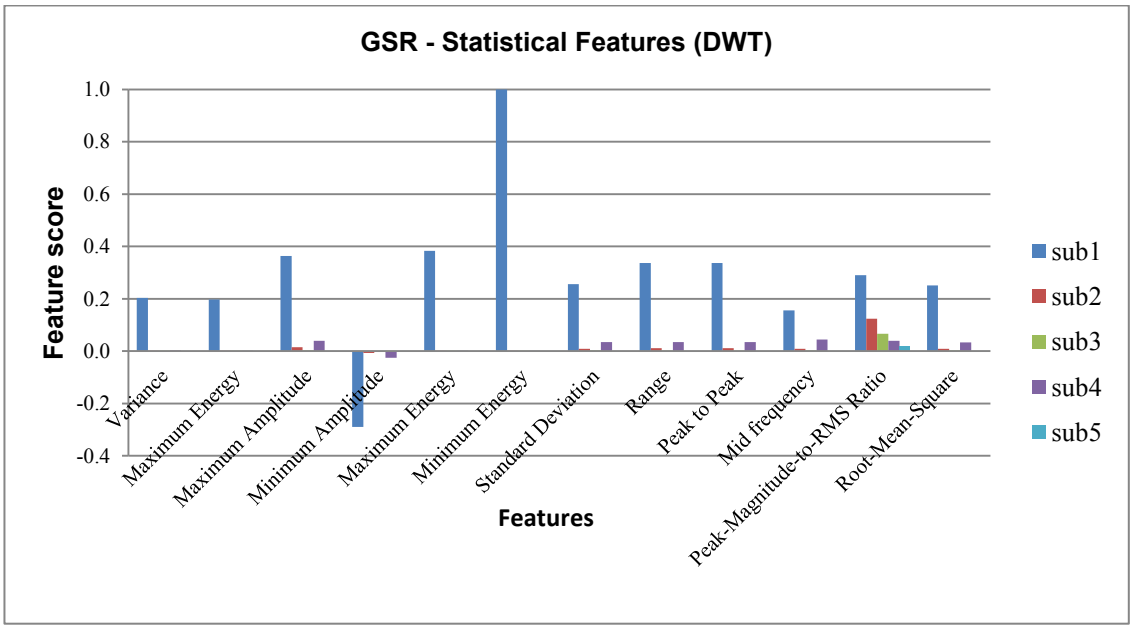


Figure 4. 15: Statistical Feature extracted from GSR from all subjects

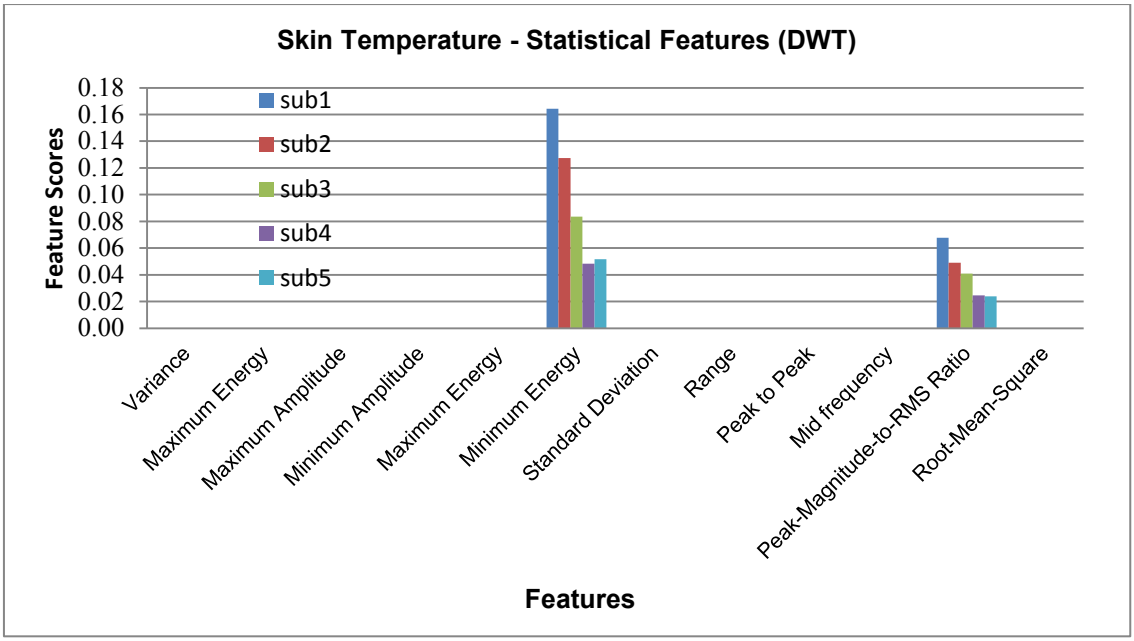


Figure 4. 16: Statistical Feature extracted from Skin Temperature from all subjects.

The skin temperature has just two features that could discriminate subjects and the remaining features had no enough output to discriminate the subjects. On the other hand, the wavelet entropy features has useful information to discriminate the five subjects as seen in Figure 4.17 and 4. 18. From the graphical interpretation, the skin temperature has shown more discriminatory information than the GSR however fusion of the two modalities will reduce the user authentication equal error rate.

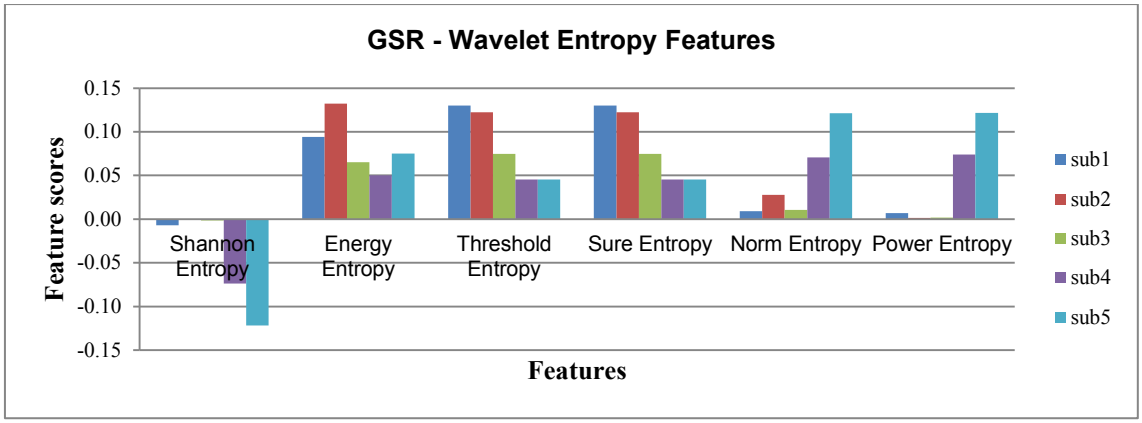


Figure 4. 17: Wavelet Entropy extracted from GSR from all subjects.

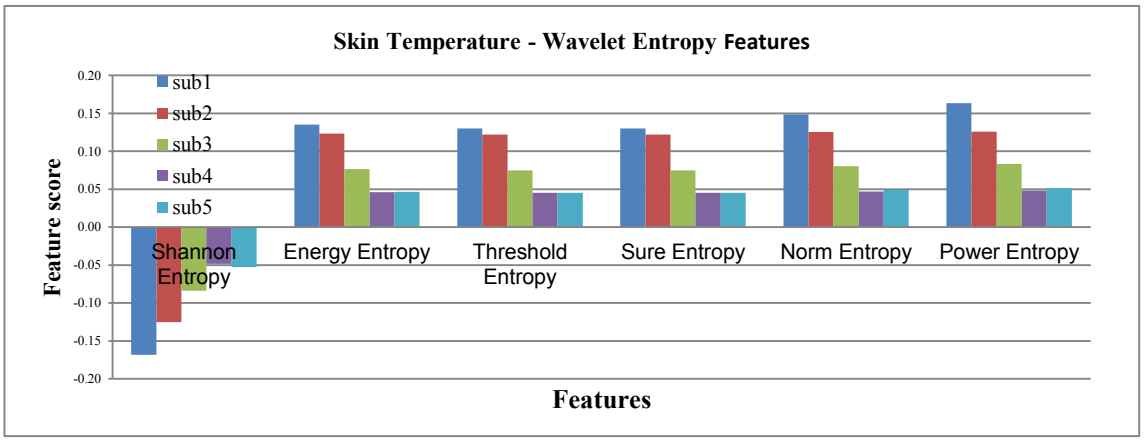


Figure 4. 18: Wavelet Entropy extracted from Skin Temperature from all subjects.

The six features from the wavelet packet entropy have shown its ability to extract most of the signal energy for effective representation which is an advantage of wavelet entropy (Varanis and Pederiva, 2015). Using MATLAB (wentropy), the Shannon entropy, energy entropy, threshold entropy, sure entropy, norm entropy and power entropy were computed to extract the features (Reiss and Stricker, 2012).

4.4 Transparent Authentication: Utilising Heart Rate for User Authentication

The secession answers the last research question of the suitability of the extracted features to successfully discriminate subjects to achieve an acceptable identification rate. To

achieve this, a preliminary experiment is presented using heart rate for user authentication. It provides a base line experiment for the rest of the experiments on transparent and continuous user authentication. The proposed idea is based on the premises that the performance of the heart rate for user authentication will set the minimum performance result for comparison. The first step in the process is to segment the signal into smaller segments using time frames. The selected statistical features are extracted from each segment of the heart rate signal using DWT.

4.4.1 Heart Rate Dataset

The goal in this research is to use a dataset that capture the natural activity of each user. In the process of extracting the data, there are some issues faced. As expected in a real-life scenario, the possibility of environmental interference like noise (i.e. wireless and other Bluetooth connection) is expected. The process of the data extraction includes the combination of different third-party applications installed on the phone to successfully extract the biometric data. This is done to overcome intrusiveness when the data are collected for the implementation of the authentication process. Three applications are integration to do different functions within the mobile device as described in Section 4.2.4. One of the issues faced is the sampling rate that can be set at 16 Hz, 32Hz and 64Hz with the default rate at 16 Hz. Due to android issues, the sampling rate setting can return to the default rate at the start of each extraction, therefore the sampling rate left at the default sampling rate.

The dataset is made up of the heart rate for 1 hour resulting in 3,600 seconds of bioelectrical signal extraction from 30 subjects. The 30 subjects are selected Centre for Security, Communication and Network (CSCAN) research, University of Plymouth. The dataset extraction is not a controlled one therefore, subjects are expected to include activities like sitting, walking and sitting within the data extraction duration. The heart rate

signal is pre-process by segmenting it into 60 seconds per segment, this translated to 60 segments per subject. Other information on the dataset is shown in Table 4.3.

Table 4. 3: **Heart rate for user authentication data information**

Data information	
Bioelectrical signal	Heart Rate
Activity	Uncontrolled activity
Number of subjects	30
Features extracted	The variance, minimum amplitude, maximum energy, standard deviation, maximum amplitude, peak2peak, peak magnitude to RMS ratio, average frequency, root mean square (RMS) and peak magnitude

4.4.2 Heart Rate Signal Feature Extraction

After establishing the features to use, the work applied the features selected for experiment two. The ten statistical features are used to study the discrepancy between the 30 subjects. The extraction of the statistical features is done after the signal has been decomposed using biorthogonal wavelet transform into 4 sub-bands of Detail coefficient and Approximation coefficients as illustrated in Figure 4.19. The Biorthogonal wavelet (a family of wavelet transform) includes Bior1.1, 1.3, 1.5, Bior2.2, 2.4, 2.6, 2.8, Bior3.1, 3.3, 3.5, 3.7, 3.9, Bior4.4, Bior5.5 and Bior6.8. The features are extracted from each of the sub-bands of the detail coefficient of bior4.4. The feature extraction experiment is executed using MATLAB script which is shown in Appendix C.

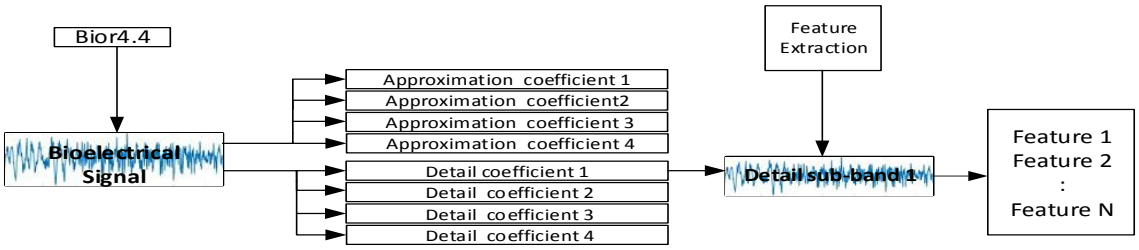


Figure 4. 19: Feature extraction procedure

The heart rate bioelectrical signal from the one-hour dataset is used for this experiment for 30 subjects. This experiment is to evaluate the effectiveness of the feature extracted in the different sub-bands and selected the most suitable sub-band to use for the rest of the experiment for the heart rate and other bioelectrical signals. The feature classification is a crucial aspect of pattern recognition. The experiment used Neural Network-Feedforward (NN-FF) for the classification. As stated earlier, NN-FF can perform better in nonlinear statistical modelling. Therefore suitable for use in the classification bioelectrical signals. Ten statistical features that were selected are extracted using the discrete wavelet transform after decomposing the bioelectrical signal using biorthogonal wavelet (boir4.4). This is only applied to the heart rate bioelectrical signals. Figure 4.20 illustrates the decomposition of the signal using biorthogonal 4.4 (Bior4.4) to decompose the signal into four levels of detail (D1-D4) coefficient.

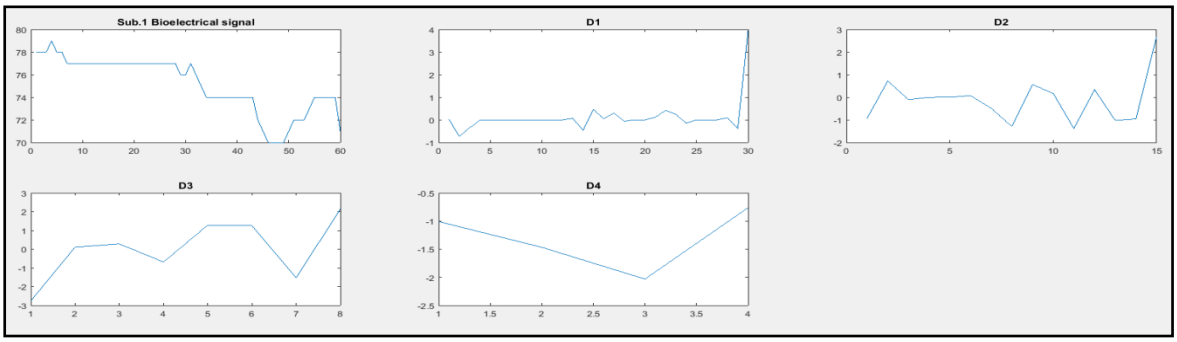


Figure 4. 20: Four levels of decomposition applying biorthogonal wavelet (bior4.4) showing the detail coefficient of the signal at the four levels D1–D4

4.4.3 Heart Rate Signal Classification Result

This experiment is a pilot experiment to verifying the discrimination of subject using one bioelectrical signal of the heart rate to obtain the best level of sub-band decomposition to use for the rest of the experiment. The result from the 30 subjects after using NN-FF classifier for the four sub-bands are encouraging as illustrated in Figure 4.21. The use of

statistical features achieved 17.2% EER at the first level of the sub-band that is the best result and 21.8 % at the fourth level as the worst. This might be due to the discrimination information available within the first level. The continuous reduction as the level increases does not mean that all subjects performed badly at the individual rate.

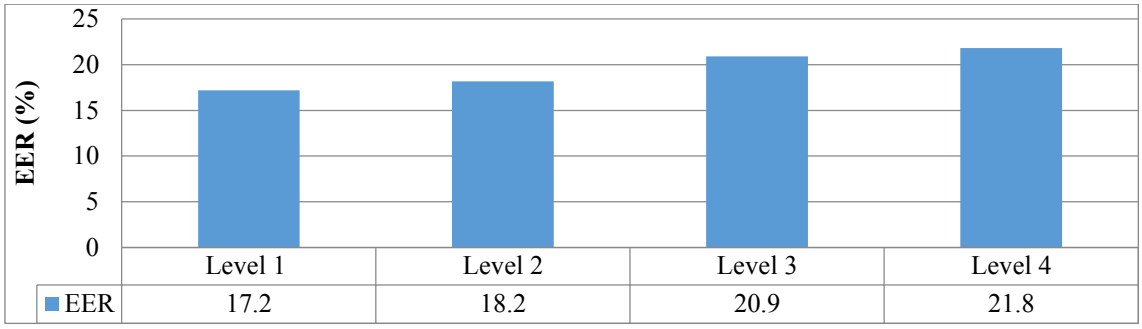


Figure 4. 21: The EER sub-band classifications of subjects from level 1 to 4.

The EER of individual results across the four levels of sub-band shows that individual's performance varies depending on the levels therefore fusion of the feature is undertaken to improve the result. The fusion is done after extracting the feature at various levels. The features are first normalized at each level before the fusion is done. The result at the fusion level has shown an improved EER of 11.25%.

Table 4.4 shows the performance between subjects at the different levels of the sub-band. The best individual performance at the first level is subject 5 with an EER of 0.6%, best at the second level is subject 4 with EER of 4.1%. Subject 20 has the best performance at the third and fourth levels with EER's of 7.9% and 10.6% respectively. This mean performance cuts across difference sub-band levels. It will be ideal to achieve a system performance of EER below 10% for the system that some subjects achieved. The performance of individual subjects achieving below the EER of 10 % cut across all levels. At this point of the experiment just one bioelectrical signal is used, therefore if it achieved

10% or below 10% EER after fusion of more bioelectrical signals it is expected to reduce further. In level one, six subjects achieved less than 10% while four subjects recorded below 10%at Level two. Level three shows two subjects scored below 10% and level four has none though subject 20 achieved 10.6%, which is closest to the expected mark.

Table 4. 4: Results of EER of Subjects at different levels of the sub-band

Subject's EER result at different levels (%)													
ID	**Level**				**ID**	**Level**				**ID**	**Level**			
	1	2	3	4		1	2	3	4		1	2	3	4
1	9.3	24.0	24.6	25.9	**11**	22.6	12.4	20.6	25.1	**21**	21.4	28.7	26.4	26.9
2	20.5	15.7	11.0	14.8	**12**	8.9	24.6	29.9	32.3	**22**	31.8	20.9	40.7	30.1
3	14.0	21.6	15.5	12.9	**13**	16.3	22.5	21.8	21.6	**23**	39.4	25.1	30.3	36.1
4	14.1	4.1	8.8	11.8	**14**	23.0	23.0	24.2	17.0	**24**	27.7	10.4	14.5	14.8
5	0.6	11.0	25.4	12.6	**15**	15.6	17.7	19.6	19.2	**25**	12.8	17.6	28.3	24.1
6	16.3	13.7	20.6	22.8	**16**	20.1	12.1	17.9	15.6	**26**	12.5	31.0	21.0	25.6
7	23.7	16.7	16.4	21.5	**17**	9.2	23.0	14.7	16.0	**27**	15.5	16.6	19.7	19.1
8	16.6	11.8	11.8	17.0	**18**	18.6	32.9	21.0	15.4	**28**	14.9	9.4	18.5	46.6
9	25.8	31.7	40.8	29.0	**19**	8.3	20.8	21.1	24.8	**29**	7.4	17.7	23.9	22.4
10	17.2	8.5	18.3	31.2	**20**	15.2	12.2	7.9	10.6	**30**	16.7	7.9	12.3	12.1

The use of multiple sample of a biometric can add value to the result but it can also have implications depending on the dataset (Atrey et al., 2010). Fusion of biometric is done at different levels, the feature extraction level, match score level; and the decision level. To improve the classification result, the four levels of decomposition are fused after the features are extraction and the results showed an improved EER of 11.25%. This is an improvement of 5.95% after the combination of the decomposed signal feature as illustrated in Figure 4.22.

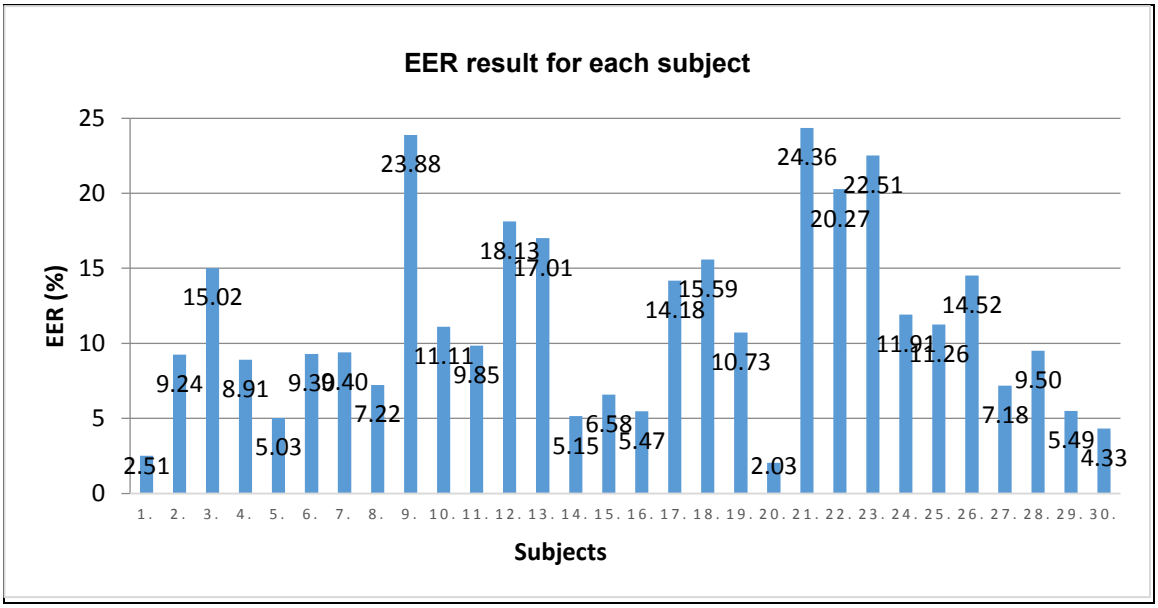


Figure 4. 22: Showing classification result of all 4 levels individually

The experiment showed different subjects performed differently depending on the sub-band levels and the sub-band fusion classifications. Some subjects performed well on both while others on only one of the classification. It is expected that with the fusion of the sub-band, there should be improvement across all subjects above the best in the sub-band performance. This is not the case, from the result of the sub-band fusion; it shows more subjects perform better on the fused result while some unexpectedly performed better on one or two of the sub-band like subject 18, 22. This is seen in subject 3's performance, there is little change in the sub-band fusion classification where they scored 15.02% EER that is almost the same on the 3 level sub-band results at 15.50% EER. It has a better result at level 4 scoring 12.9% EER compared to the sub-band fusion with 15.02% EER. The same is for subject 10 with the best result on level 1 at 8.5% EER compared to the sub-band fusion at 11.11% EER. Other subjects scoring the best result at level 1 of the sub-band level include subject 12 scoring 8.90% EER compared to sub-band fusion scoring 18.13% EER, subject 13 at 16.3% EER (sub-band fusion 17.1% EER), subject 17 at 9.2% EER (sub-band fusion 14.18% EER), subject 19 at 8.3% EER (sub-band fusion 10.73%),

subject 21 at 21.4% EER (sub-band fusion 24.36% EER) and subject 26 at 12.5% EER (sub-band fusion 14.52 % EER). The best results at the sub-band level 2 include subject 24 at 10.4% EER and subject 28 at 9.4% EER compared to the scoring at the sub-band fusion at 11.91% EER and 9.5% EER respectively. At Level 4, only subject 18 recorded their best performances at 15.4% EER compare to sub-band fusion at 15.59% EER. In term of individual performance, the fusion of all levels has shown to be effective in discrimination of subjects. 60% of individual results improved with the fusion introduced. While 40% of the subjects scored a better EER at the sub-band level. The best for each of them showed that subject 4 scored 8.8% EER, 12 (8.9% EER), 17 (9.2% EER), 19 (8.3% EER) at the 1st level, 2nd level have subject 10 scoring 8.5% EER, 28 (9.4% EER). These subjects individually performed below the expected 10% of EER. This brings to a total of subjects scoring below 10% of EER across the sub-band and the fusion classification to about 66%.

4.5 Conclusion

From the first to the fourth experiment it shows the potentials in the procedure of the use of bioelectrical signal in achieving the aim of the research goal. The use of a single bioelectrical signal for the classification set the stage with encouraging result. The use of bioelectrical signals for user authentication in this research has proven to be discriminatory between subjects. Thought the unimodal of the heart rate bioelectrical signal had a relatively good performance using biorthogonal wavelet to decompose the bioelectrical signal into four sub-bands. The best sub-ban achieved 17.2% EER. The fusion of the four sub-band improve the result with more than 83% have above 17.2% afterword. The use of unimodal bioelectrical signal proves to be effective but not sufficient. This is because the output result is still on the high side that mean more genuine subjects will be rejected.

Therefore, to optimize the system by employing more than one classifier will enhance the overall goal of the research.

5. Classification and Optimization of Bioelectrical Signal for User Authentication

To optimise the biometrical authentication system, more than one classifier will be used for comparison. The classification will involve two classifiers at the first instance with the aim of using the best classifier for the finals classification of the subjects. The classifiers proposed for comparison includes Random forest and Neural Network. The Random forest and Neural Network classification methods will further be discussed in the section for classification. To optimize the system for user authentication improvement, an algorithmic approach is adopted applying the extracted data based on the subject's activity when the data is extracted. To successfully carry out the research aim of this chapter, the extracted data is divided into three categories; bioelectrical signals, context awareness data and the subject's activity information. The different processes are further discussed in details in the following section.

5.1 Introduction

The previous chapter has established the viability of using bioelectrical signals of the heart rate for authenticating a subject. The experimental work applied Wavelet Transform using both Discreet Wavelet Transform (DWT) and Wavelet Packet Entropy (WPE) to extract the features before classifying the extracted feature template. The use of one bioelectrical signal might be limit discrimination but with more bioelectrical signals, the discrimination of subjects will improve. Another aspect of the experiment is the segmentation (which was not use in the previous chapter) of the signal for a continuous user authentication. Therefore, to improve upon the achievement in chapter 4, this chapter will focus on:

- The collection and used of a dataset that will take into account the subject's daily activity. That means the subject will not be subjected to any pre-defined action or

activity but expects the subject to go about his/her daily routine while the data is extracted.

- The selection of the most suitable timeframe window for segmenting the data that could contain useful discriminatory information for authenticating a subject
- Applying the most suitable classifier to maximally achieve a better classification output.
- Establishment of a suitable approach for fusing the extracted features and contextual data to create a unique template as an input vector for classification.
- Creation of a suitable multi-algorithmic approach for optimizing the classification of the subject to attain an efficient user authentication system. To optimize the bioelectrical signals for user authentication, other processes will be included including segmentation of the signals, selection of classifier and creation of algorithms. These processes will be analysed in detail in different sections of this chapter.

5.2 Data Segmentation

5.2.1 Dataset

It is apparent that the use of a single bioelectrical signal in the prior work is not adequate in meeting the anticipated result. Research has shown that the use of more than one biometric in an authentication system improves the security level because it increases the biometric representation (Ambalakat, 2005). Bioelectrical signals can also be affected by the emotional state or the heath of the subject (Lee and Hsieh, 2014, Bono et al., 2016, Gomez et al., 2016). The data set used in this part of the work is a new set of dataset extracted for a duration of four hours from 30 subjects over seven days which is more than the dataset used in Section 4.4. In Section 4.4 only the heart is extracted for one hour only

while more than one bioelectrical signal is used for this experiment. The population of participants are selected from the university community with age between 18 and 40 as shown in Table 5.2. The bioelectrical signals used for this experiment also include Heart Rate (HR), Galvanic Skin Response (GSR) and Skin Temperature (ST) as illustrate in Table 5.1. To increase the performance of the subject's identification applying context awareness will increase it. Therefore, two context awareness information altitude and steps is fused to the bioelectrical signal. The total number of subjects is 30 and the bioelectrical signals and context awareness data were extracted for duration of 100,800 seconds see 4.2.4. The study dataset composition is shown in Table 5.2 with the data application information.

Table 5. 1: The selected information from the dataset file

Data Type	Data Information	Data application
Bioelectrical signal	Heart Rate	Feature extraction
Bioelectrical signal	Heart Rate Variability	Feature extraction
Bioelectrical signal	Skin Temperature	Feature extraction
Context awareness	Altitude (ascending and descending)	Contextual information
Context awareness	Steps (pace and Speed)	Contextual information
Activity Information	Sitting, Standing and Sleeping, Walking, Jogging, and Running	Activity analysing

Table 5. 2: Dataset Participant Composition

Age group	Male	Female	Total
18 - 25	8	3	11
25-30	6	0	6
30 - 35	3	1	4
35 - 40	6	2	8
40 - Above	1	0	1
Total	24	6	30

The experimental dataset for this chapter is for a significant longer period of four hours over seven days in total to establish a physiological pattern for each user. The data extraction is restricted to 7 days, 4 hours per day due to some issues discussed in the

previous chapter see Heart Rate Dataset page 73. The data collection lasted for more than three months and was concluded in June 2017. 30 subjects from the University of Plymouth participated in the data extraction after ethical approval has been approved. This translates to 100,800 seconds for each of the 30 subjects. For the experiment data, several bioelectrical signals and subject's contextual activities as shown in Table 5.1 is used. It should be noted that no pre-determined activity was defined to be carried out during the data extraction but subjects were to carry on with their daily routine while the recording is taking place. Also, the Heart Rate Variability (HRV) is extracted with other bioelectrical signals but was not

5.2.2 Segment Selection

The segmentation of the dataset is important for the successful classification of the subjects. Therefore, this section will answer the research question on the best timeframe for segmenting the bioelectrical signal that could contain enough information within the segmented samples for verifying a subject. The application of appropriate features to use for the remaining part of the experiment for heart rate has been provided in the last section experiment. The first Level of the approximation detail coefficient has shown to be the best feature set to use as shown in the preliminary experiment. For this experiment, the dataset is recorded for a longer time of four hours a day for seven days with subjects going normal daily activities. The data file contains several bioelectrical signals but only the heart rate will be used for the experiment. For the authentication window, each subject's signal is segmented into time frames of seconds (Georgoulas et al., 2005). The time window is to determine the best window that a user can be accurately authentication considering that the authentication is continuous. Authentication system reliability is expected to be high and as much as possible fast too. A faster authentication process is

more suitable for users because it gives genuine user prompt access, therefore three-time window of 3, 5 and 10 seconds compared to the used of 60 seconds used in the preliminary experiment using heart rate only. Table 5.3 shows the data information with the total amount of segment for each time frame.

Table 5. 3: Showing heart rate data information on 30 subjects recorded for 4 hours over seven days

Bioelectrical signal	HR, GSR and ST		
Data Types	3 Seconds	5 Seconds	10 Seconds
Sampling rate	8	8	8
Data points per segment	24	40	80
Number of Feature Segments of each Subject	4800	2880	1440

The EER result in Figure 5.1 shows the 3 seconds time frame to be the best. The EER results from the classification are not the best that can be obtain from it. A network size of 20 is used across all the signals. The speed (pedometer) and altitude (altimeter) results showed the 3 performed better than 5 seconds did. Though three segments were used but it became unnecessary to include time frame of 10 seconds that is the worst of the three. The 3 seconds time frame is the best EER on the all the experiment but for comparison segment 3 and 5 is shown in Figure 5.1-5.3

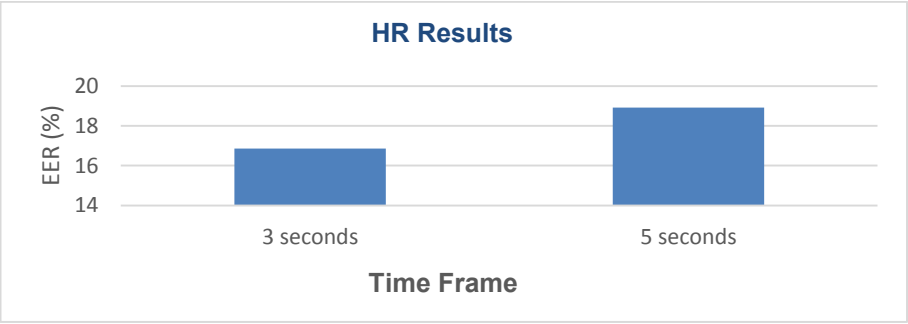


Figure 5. 1: Showing different time segments and their EER results of the heart rate.

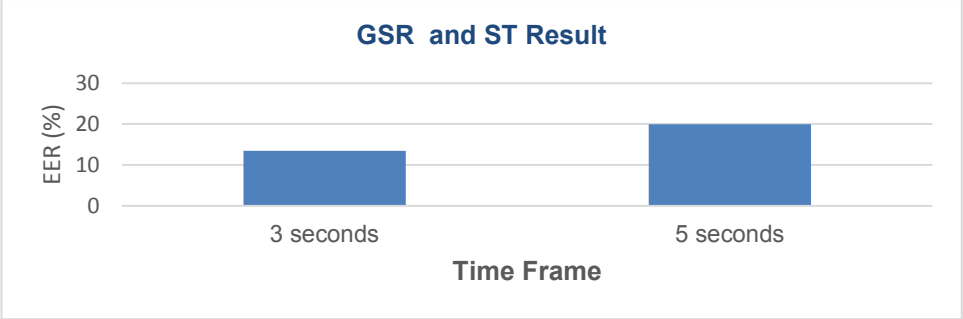


Figure 5. 2: Showing different time segments and their EER results of the GSR and ST

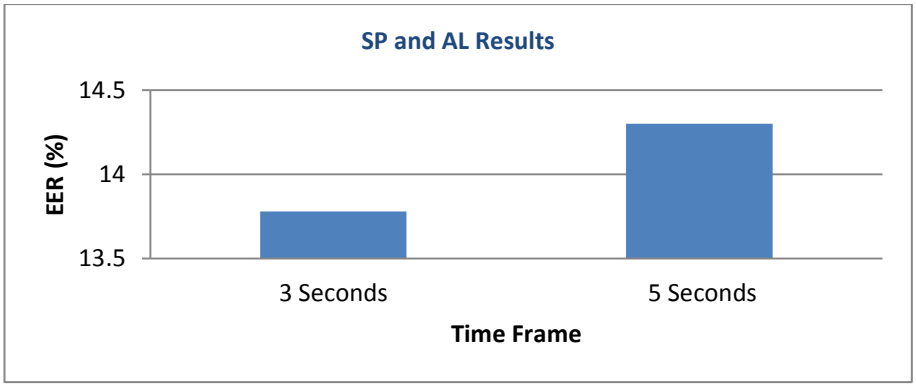


Figure 5. 3: Showing different time segments and their EER results of Pedometer and Altimeter

The experiment on the selection of time frame achieved a promising result because all the bioelectrical signals with 3 second time frames are the best. More interesting is the fact the pedometer and altimeter data had 3 seconds time frame as the best time frame too. This shows the viability of the use of bioelectrical signal for continues user authentication within a short time frame. The faster the authentication process the better the system for transparent and quick acceptance of genuine subjects while rejecting impostors. To further analysis the time frame classification output, the best performance is accessed on individual bases across the three classifications as illustrated in Figure 5.4.

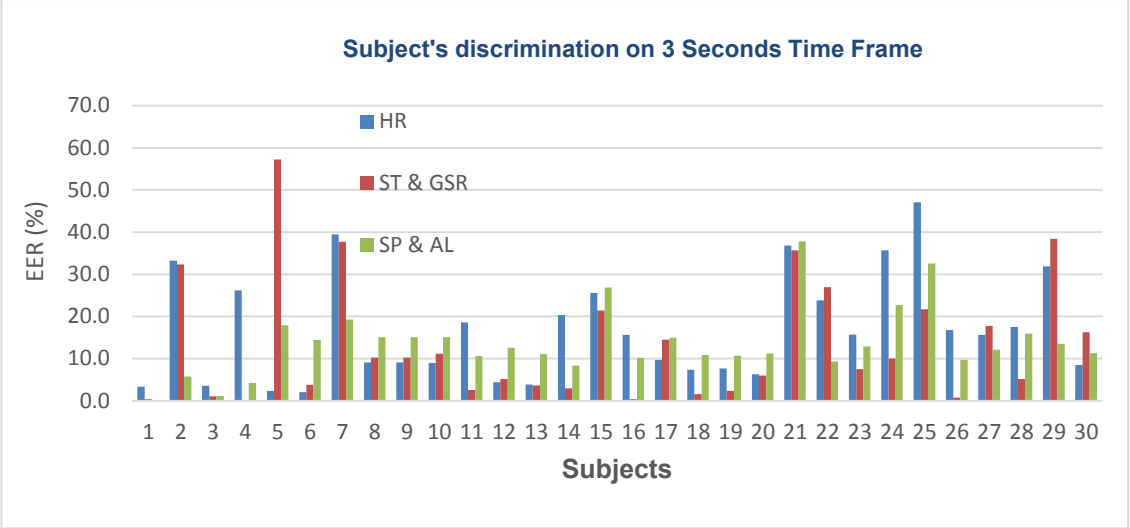


Figure 5. 4: Subject's discrimination on 3 Seconds Time Frame

The classification of the three-different data of Heart Rate (HR), Skin Temperature (ST) and Galvanic Skin Response (GSR) and Step and Pace (SP) and Altitude (AL) shows different subjects performing on different data set. 7 subjects performed better on the HR dataset compare to other dataset while 17 subjects have their best with the ST and GSR and the SP and AL have 6 subjects having the best performance on the 3 second classification. The best and worst subjects' EER performance from the 3 second and 5 seconds are compared between the three classifications illustrated in Table 5.4 and 5.5

Table 5. 4: The 5 best and worst Performances of 3 second time frame

Subject ID	5 Best Performances in EER (%) for 3 Seconds			Subject ID	5 Worst Performances in EER (%)for 3 Seconds		
	HR	ST & GSR	SP & AL		HR	ST & GSR	SP & AL
1	3.33	0.39	0.07	**5**	2.34	57.22	17.9
3	3.54	1.05	1.11	**7**	39.45	37.69	19.25
6	2.07	3.82	14.45	**21**	36.83	35.67	37.76
13	3.90	3.61	11.07	**25**	47.05	21.74	32.57
18	7.34	1.60	10.83	**29**	31.86	38.43	13.51

Table 5. 3: The 5 best and worst Performances of 5 second time frame

Subject ID	5 Best Performances in EER (%) for 5 Seconds			Subject ID	5 Worst Performances in EER (%) for 5 Seconds		
	HR	ST & GSR	SP & AL		HR	ST & GSR	SP & AL
1	6.46	7.74	0.09	**5**	17.67	23.01	17.67
3	5.40	6.10	3.88	**7**	19.34	24.84	19.34
6	2.73	21.23	14.40	**21**	36.04	23.48	36.04
13	18.78	20.27	11.16	**25**	32.25	19.69	32.25
18	13.08	12.93	11.40	**29**	17.61	35.79	17.61

The five best performances from the 3 second time frame shows 4 subjects form the ST and GSR have the best among three datasets. Subject 1 on the SP and AL dataset is the fifth subject with the best leaving the HR rate without any. For the worst performance, only subject 5 performed below 10% from the HR classification. The HR has two having the worst from the five subjects while ST and GSR and SP and AL have two and one subjects respectively among the worst performance. The HR has the worst performance base on the five best and worst performance analyses. This could be attributed to amount of discrimination information contain in the dataset. The HR contains just the heart rate bioelectrical signal while the rest of the dataset contain for the ST and GSR the skin temperature and the galvanic skin response bioelectrical signals while the SP and AL contain the speed and attitude contextual dataset. To go further on the research, the 3 second time frame will be used across all the extracted bioelectrical signal and contextual information for segmentation.

5.2.3 Discussion

The use of different time frames help to identify the best duration for an authentication to be processed. This has helped to know the most effective duration in time the signal can be segmented to increase the discrimination level of subjects. The classification result shows about 26.7% of the subjects that includes subject 5, 6, 8, 9, 10, 12, 17, and 30 for the 3 seconds time frame classification. The 5 seconds time frame classification has 8 subjects performing better with the heart rate. It could also be seen that subject 6, 8, 9 10, 12 and 17 share the same performance across the time frame classifications. Therefore, it will be suggestive that those subjects that have better performance across both time frame classifications contain better discriminatory information in their HR template than the other dataset. The ST and GSR result achieved a slightly better performance over the contextual data in the 3 seconds time frame result. Table 4.5 and 4.6 shows the best result

from the 3 seconds time frame classification achieved better than the 5 seconds time frame except for subject 6 on the speed and altitude. On the subject's worst performance of the 3 seconds time frame, the corresponding 5 seconds time frame however performed better except for subject 5 achieving 2.34% EER on the heart rate and subject 29 achieving 13.51% EER on the Speed and Altitude. The segmentation using the time frame 3 seconds has shown to be more discriminatory than the other time frames used but more interesting is the fact that the shorter the time the better its usefulness for faster authentication process. This is because it takes a short time (3 seconds per sample) to generate biometric samples for authentication. Therefore, a short time frames to extract information for authentication which in turn reducing the time it takes for rejecting an illegitimate subject. It is expected for the worse result to achieve high rate of rejecting legitimate subjects therefore, fusion of the signal and contextual data will increase information content and possible increase the discrimination level. The use of multi-algorithm approach will perform significantly better than using a single algorithm. Therefore, a multi-algorithm approach will be considered to improve the user authentication system. Therefore, to improve on the result of the unimodal of the bioelectrical signal of the heart rate, more signals were introduced and fused together after the features are extracted to improve the result. The study investigated the best time frame to use for segmenting the signal. The result showed that the lower the time frame, the better the performance. The use of the best time frame for feature extraction before fusing the features and contextual information for classification will form the basis for the next chapter.

5.3 Classification Optimization

To achieve the above aim, sufficient dataset is required for thorough investigation of the nature of the classifiers to enable optimization. As stated earlier, the feature extraction is

done on each of the bioelectrical signal before fusion with the contextual information for classification. The multi-algorithm approach is implemented to maximise the use of the fused output to classify a subject. The advantage of this approach is that it solves some limitation faced by some biometric system. The subject will not be involved in the authentication process that makes it non-intrusive and convenient for the subject.

The classification is expected to achieve a maximum result good enough or better compared to other research work discussed in chapter three. The classification will involve two classifiers with the aim of using the best classifier for the finals classification of the work. Random forest and Neural Network is proposed for used in the chapter.

5.3.1 Dataset

It is apparent that the use of a single bioelectrical signal in the prior work is not adequate in meeting the anticipated result. Research has shown that the use of more than one biometric in an authentication system improves the security level by increasing the biometric representation (Ambalakat, 2005). Bioelectrical signals can also be affected by the emotional state or the heath of the subject (Lee and Hsieh, 2014, Bono et al., 2016, Gomez et al., 2016). Therefore, including more bioelectrical signals will improve the information available for discrimination of subject. The heart rate variability that was not used in the previous experiment is included to increase the bioelectrical signals to four as shown in Table 5.6. The heart rate variability contain the same characteristic with the heart rate therefore, the features used for the heart rate is applied to the HRV. To successfully carry out the research aim of this chapter, the extracted data is divided into three categories; bioelectrical signals, context awareness data and the subject's activity information. The study dataset composition is shown in Table 5.6 with the data application information. The data is extracted for 30 subjects, 4 hours over 7 days to arrive at a

reasonable quantity of information available for the experiments. The method of extraction is the same as the last experiment data extraction see 4.2.4 page 60.

Table 5. 6: The selected information from the dataset file

Data Type	Data Information	Data application
Bioelectrical signal	Heart Rate	Feature extraction
Bioelectrical signal	Heart Rate Variability	Feature extraction
Bioelectrical signal	Galvanic Skin Response	Feature extraction
Bioelectrical signal	Skin Temperature	Feature extraction
Context	Altitude (ascending and descending)	Contextual information
Context	Steps (pace and Speed)	Contextual information
Activity	Sitting, Standing, Sleeping, Walking, Jogging, and Running	Activity analysing

5.3.2 Features Used

The features are extracted from each bioelectrical signal separately. The heart rate (HR) and heart rate variability (HRV) used the same features set each while the skin temperature (ST) and the Galvanic Skin Response (GSR) used the same as described in the previous chapter. Each of the bioelectrical features extracted are normalised between figures 0 to 1. A total of ten features are used for the HR and HRV while the ST and GSR used six features each as shown in Table 5.7. The basis for using few numbers of features predicated on the fact that mobile device power requirement is limited in capacity (Carroll and Heiser, 2010).

Table 5. 4: table showing the features extracted from each of the bioelectrical signal

Num.	HR and HRV	Num.	HR and HRV	Num.	GSR and ST
1	Variance	**7**	Peak magnitude to RMS ratio	**1**	Shannon Entropy
2	Minimum Amplitude	**8**	Average Frequency	**2**	Energy Entropy
3	Maximum Energy	**9**	Root Mean Square (RMS)	**3**	Threshold Entropy
4	Standard Deviation	**10**	Peak Magnitude	**4**	Sure Entropy
5	Maximum Amplitude			**5**	Normalized Entropy
6	Peak2peak			**6**	Power Entropy

5.3.3 Biometric Fusion Template

The fusion of modalities in a biometric system plays a vital role in improving the level of security of the system. The fusion of modalities is used to solve the drawback of using single biometric which enhances the user authentication (Indovina et al., 2003). It

increases confidentiality and the available options for the authentication mechanism. The fusion of modalities are in three stages the early, intermediate or the later stage of the process (Bubeck, 2003, Kisku et al., 2009).

- **Fusion at the feature extraction level**: The fusion at this level is done by concatenation of the features extracted into one feature vector.
- **Fusion at the matching scores level:** The fusion uses each extracted feature as a separate vector. Each feature vector is score differently with best scores combined to achieve a better result.
- **Fusion at the decision level:** in this level of fusion, the features are classified, and the classification result is presented as accept or reject. A majority vote is employed to make the final decision as this increases the reliability of the system (Zuev and Ivanov, 1999).

Fusion at the feature extraction level is used for this work. The fusion mechanism is done in two ways. First, the normalised features of each subject's bioelectrical signal are fused into one matrix. The feature matrix is later fused with subject's context awareness information. The context awareness data is expected to increase the information discrepancy between subjects to improve the classification result. Also taking computational power awareness into consideration, the application of fusion at the feature level and the fusing of context awareness data before classification is to reduce the power consumed during classification. The classification of each signal feature set separately will increase the system power consumption.

5.3.4 Classification

In this chapter, the focus has been on the optimization of the of the user authentication system. The use of multi-biometric approach in the feature extraction was discussed in

chapter 4. To improve on the results, multiple approaches are applied to enhance and optimize the performance of the entire system. To compare the multi-modal performance, two classifiers are used to classify the fused feature template of the bioelectrical signal and contextual information. The analysis of the experiment using a static network size for the classification of the feature template has shown potential in the use of bioelectrical signal. Therefore, different network sizes are used for classification of subject at this stage.

In addition to feed-forward neural network used in the prior experiment, random forest is included in the classification of the feature template for comparison. Previous studies have used random forest for classifying signals (Liaw and Wiener, 2002, Breiman, 1999). Random forest can improve the accuracy of a signal classification by using a voting system to identify the most suitable class (Breiman, 2001). It is popular for classifying bioelectrical signals like EEG and biomedicine and has shown to be effective and robust for classification (Colomer Granero et al., 2016). It is based on multiple trees decision and good for large datasets and databases classification (Belle et al., 2012).

5.3.5 Decision

The application of recognition decision scheme after a classification is a popular way of enhancing the overall system performance of the authentication system (Battiti and Colla, 1994) and increases the reliability as stated earlier. The use of decision scheme is to improve the classification performance of the biometric system. There are varieties of decisions scheme that can be used for enhancing classification output Therefore to increase the accuracy of the classification output, a decision scheme will be decided for use in this research work. Two recognition decision schemes are to be discussed, these includes the weighted combining schemes and majority voting scheme.

- **Weighted Combination Scheme:** This uses some level of measurement to accept or reject the subject from accessing the system. This scheme includes such as sum-rule,

product-rule, max-rule etc. Though this scheme is has a high recognition rate but it (Tulyakov et al., 2008) but not easy in term of implementation because it involves the calculating the scores for use.

- **Majority Voting Scheme:** The use of majority voting scheme is popular among research works. This is based on applying the most number of votes above or below a threshold for accepting or rejecting the subject from gaining access into the system. The used of majority voting have some advantage which includes relatively low storage requirement for the data (Sriyananda et al., 1975). Majority is easier and straightforward to implement (Tulyakov et al., 2008) because there is no further calculation but accepting the most number above or below the threshold.

For this work majority voting will be applied because it uses low storage that is an advantage for a mobile phone because of the limited storage capacity of it. This chapter will not use majority in making decision after classification but will be referred to in the next chapters

5.4 Result

The experiment in the last chapter investigated different time frames to decide on the most suitable for segmentation of the extracted data. The 3 seconds time frame achieves the best result therefore the most suitable. In the last experiment, the aim is to select the best segment using the same network size. Therefore, this section will focus on using different network size across different network sizes for the two classifiers.

5.4.1 Methodology

The process is carries out with 30 subjects but one of the subject access the system as a legitimate user while the remaining 29 is seen as impostors. The process it done for all 30

subjects and is repeated for 10 times for each subject with the average used the classification output. The two classifiers of random forest and feedforward neutral network are used. To explore classifiers, different network sizes are used with the best network size identified. The classification of the feature template used different network size from 5 up to 100 with an interval of 5. Not all the network sizes are shown in the graph but the network sizes around the best network size showing. The details of the classifier results are presented in the result sessions.

5.4.2 Result Performance of Random Forest Classifier

The result is analysed using the Equal Error Rate as the measuring Metrix (Jayamaha et al.). The network size 35 achieves the best result for random forest with EER of 14.22% closely followed by network size with 30 and 40 neurons with EER 14.94% and 14.31% respectively. The three results are in the region of 14% with hidden neurons layer 30 to 35.

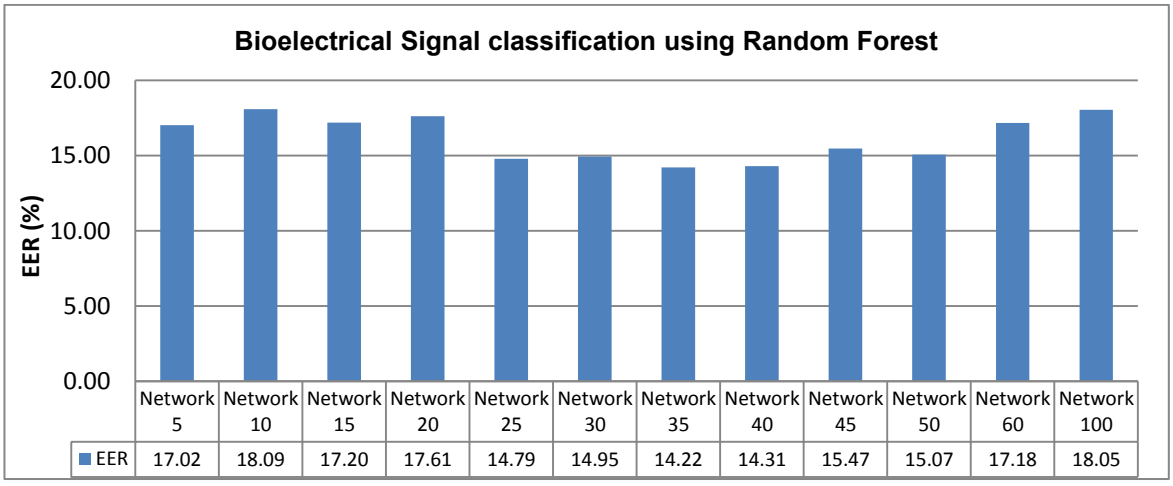


Figure 5. 5: Showing different network size and their EER results using random forest classifier

Figure 5.6 illustrates the best of random forest individual performance. The analysis of individual error rate shows subject 14 and 22 obtaining an EER of 0% as the best while the worst result is obtained by subject 24 with EER of 60.12%. With more than 43% of the

subject obtaining an EER above 10% shows that the classification using random forest performed poorly. Irrespective of the poor classifier performance, some subject achieved a reasonable result of EER less than 2% like subject 1, 3, 14, 18, 19, 22 and 26. The performance is insignificant compared with the unimodal of heart rate experiment in the last chapter using the NN-FF.

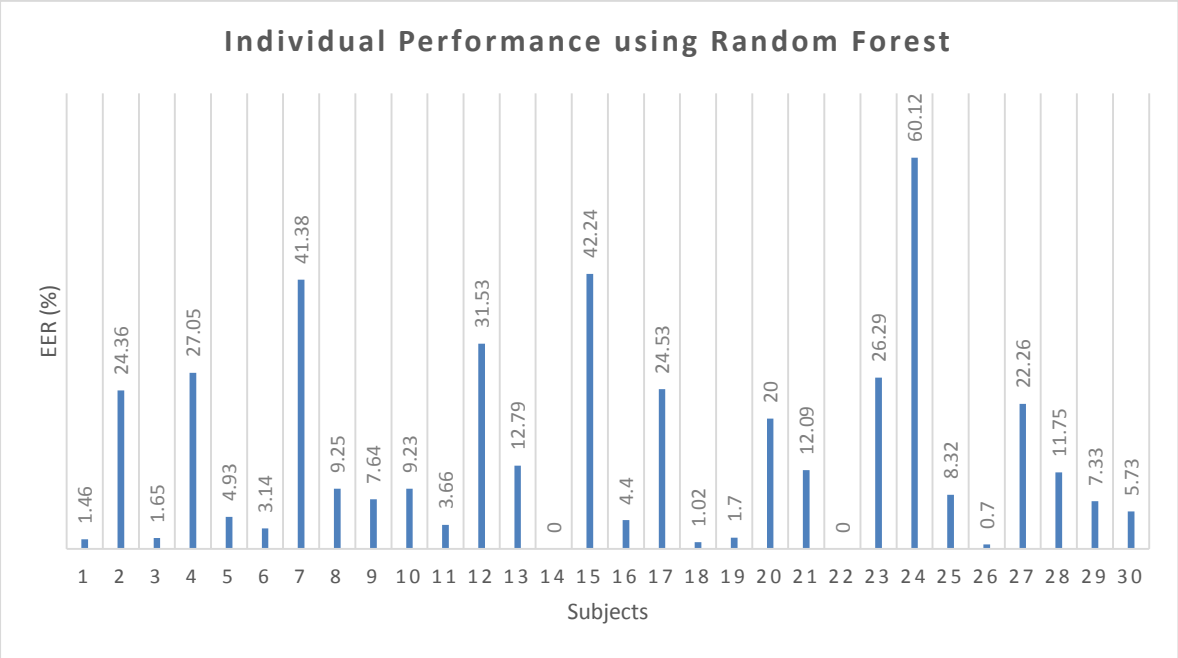


Figure 5. 6: Showing individual performance using random forest classifier

5.4.3 Performance of Neural Network Feed-Forward Classifier

Neural network as earlier discussed is popular for bioelectrical signal classification; this has been demonstrated in chapter 4. Figure 5.7 shows the result of NN-FF classifier using different network sizes. The network size with 70 neurons achieved the best performance of 3.40% compared to Random forest of EER of 14.22%. The classifiers show that NN-FF performed better than the Random forest with a difference more than EER of 10%.

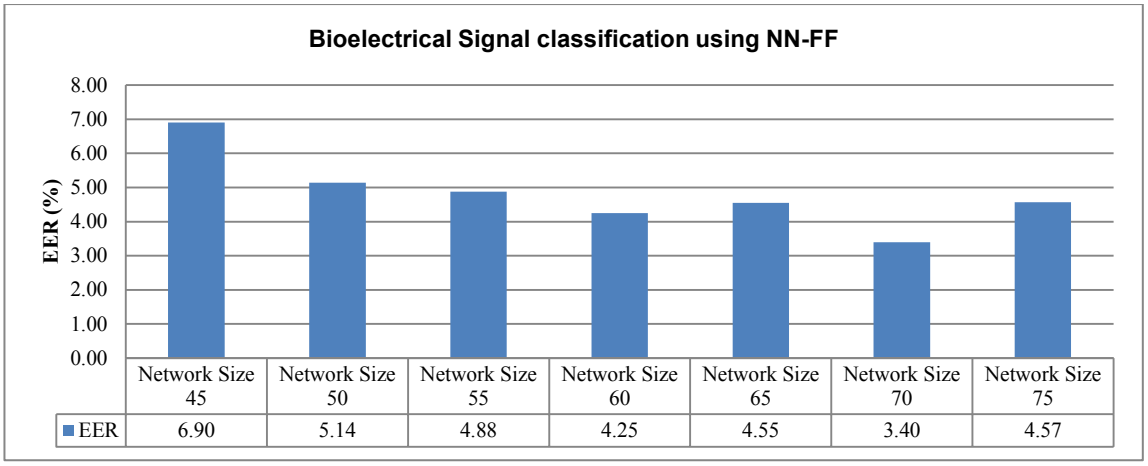


Figure 5. 7: Showing different network size and their EER results using neural network feed-forward classifier

To further analysis the NN-FF and random forest classification, the two classifiers showed a significant discrimination of the subjects. Comparing the performance of the two classifiers, only few subjects using the random forest performed better than the NN-FF classifier. These subjects include subject 6, 14, 19, 22 and 26. The random forest classifier with relative good performance to that of NN-FF are subject 1, 3, 18, 19 and 26. The NN-FF outperformed the random forest on individual performance with a difference of 10.82%. Therefore, using only one classifier will not be out of place. From the NN-FF results, the three best results are compares on individual performance as illustrated in Figure 5.8 and Table 5.8.

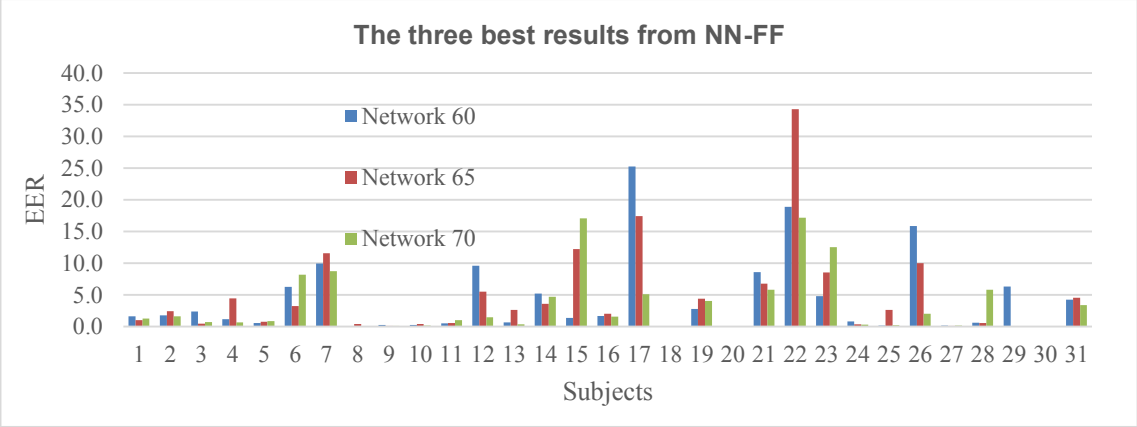


Figure 5. 8: Showing the best three network size results from neural network feed-forward classifier

Table 5. 8: Showing different the best network size EER results for 60, 65 and 70 network sizes

Classification result of network size 60, 65 and 70											
	Network Size				Network Size				Network Size		
User	60	65	70	User	60	65	70	User	60	65	70
1	1.62	1.03	1.25	11	0.52	0.56	1.00	21	8.57	6.79	5.79
2	1.79	2.41	1.63	12	9.59	5.51	1.44	22	18.92	34.31	17.17
3	2.39	0.48	0.70	13	0.67	2.64	0.33	23	4.82	8.55	12.52
4	1.16	4.44	0.64	14	5.18	3.58	4.71	24	0.83	0.35	0.28
5	0.57	0.75	0.84	15	1.36	12.24	17.07	25	0.15	2.63	0.22
6	6.26	3.26	8.17	16	1.67	2.01	1.55	26	15.88	9.99	2.02
7	9.97	11.59	8.76	17	25.25	17.41	5.09	27	0.13	0.12	0.17
8	0.00	0.42	0.01	18	0.00	0.00	0.01	28	0.61	0.57	5.79
9	0.25	0.10	0.09	19	2.79	4.38	4.06	29	6.30	0.01	0.01
10	0.28	0.40	0.18	20	0.01	0.00	0.01	30	0.03	0.04	0.06

In analysing the best three network sizes of the NN-FF, the classification shows that most of the individual performances are closely related in term of their EER. Subjects 1, 2, 5, 8, 9, 10, 11, 16, 18, 20, 24, 27 and 30 have almost the same EER across the three network sizes. Subjects 6, 15, 23 and 28 from the network size 70 scored higher EER than the other network sizes even though it has the best average performance. Subject 8,18 and 29 have the best EER of 0.01% from network with 70 neurons while subject 8 and 18 having the best EER of 0% from network 60 and subject 18 and 20 have best EER of 0% from network size 65. Subject 18 featured in all three network sizes as the best performing

subject with almost the same scores of EER. It could be seen that while the network size with 70 neurons is the best network on average, some subject performed better from the network size 60 and 65 (subject 12, 17 and 22). In general, it shows the same trend across the subjects scoring close EER across the three network sizes. Therefore, employing dynamic network size selection will not be useful for improving the classification of subjects.

5.4.4 Multi-Algorithm approach

The performance of the best network from using the NN-FF classifier from the previous section showing the subjects scoring EER of above 3.4% could be perform better if the activities are sub-divided and classified as most controlled experiments do using pre-defined activities (Shen et al., 2013). Figure 5.9 illustrate the individual performance from the best network size with an average EER of 3.4%. The analysis shows the error rates of most subjects performed better than the average performance in EER of 3.4%. About 33% of the subjects have higher EER than the 3.4% with subject 15 and 22 scoring as high as EER 17.07% and EER 17.17% respectively.

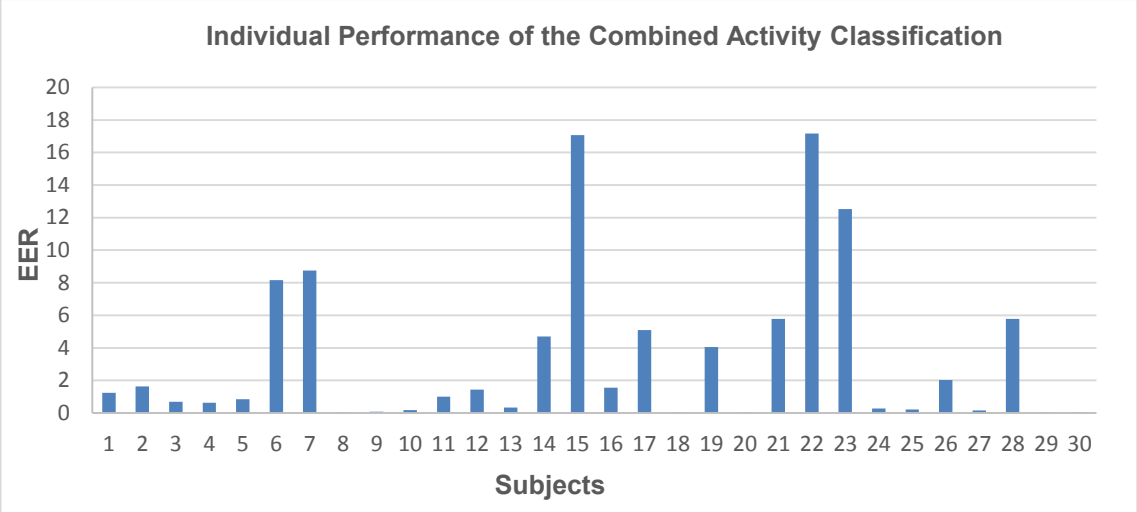


Figure 5. 9: Optimal result for each subject from the combine activity in EER

From the prior work listed in chapter 3, the worst performance is EER of 13% therefore, having a user authentication system with a performance of EER of 3.4% should be suitable for a biometric system but having 33% rejected by the system will not be ideal. To improve on the number of subjects to be accepted by the system a multi-algorithm is deliberated to improve the system. From the dataset used for this section, it will be divided into two using the activities engaged with when the subject's data is extracted. This information is logged on the data file, as the data is stored. There two additional data sub-set will be extracted from the dataset used in this section. This will lead to two additional dataset of active and non-active with the combined dataset as illustrated in Figure 5.9. The optimization of the proposed system using multiple Algorithms will be discussed in the next section.

Table 5. 9: The data sub-division for creating an algorithm

Data Type	Data information	Algorithm
Combined Activities	Walking, Jogging, Running, Sitting, Standing and Sleeping,	Combined
Active Activities	Walking, Jogging, and Running	Active
Non-Active Activities	Sitting, Standing and Sleeping,	Non-Active

5.5 Multi-Algorithm Optimization

To improve the efficiency of the user authentication system, a functional approach is expected to be applied on the system (Scheidat et al., 2006). To optimize the system, a multi-algorithm approach is adopted by dividing the bioelectrical signals into three data types. The segmentation as earlier discussed is performed with respect to the subject's activity during the extraction of the bioelectrical signals. The segmentation of the signals provides for similar characteristic with discriminatory information contain in the signal to be classed into the same segment. The rest of this section will focus on the creation and performance of the three algorithms.

5.5.1 Algorithm Creation and Classification

The dataset and features used in this section is the same as the one used in previous section. The sub-division of the bioelectrical signal and context awareness data is a first step to obtaining a reliable algorithm (Al-Waisy et al., 2015). The signals and context awareness data is divided based on the activities at the time of extraction. The sub-division of the data is automated using the activities logged in the data file as idle (non-active) or walking, running or jogging (active). Each of the bioelectrical signals and context awareness data are sub-divided into active, non-active and combined activities. Each sub-division data is segmented using the 3 seconds before features are extracted from each bioelectrical signal use the feature set as describe in the previous section depending on the type of bioelectrical signal. The first step after the features are extracted is the normalisation of the feature scores. After normalisation of the feature scores from each of the bioelectrical signal, the HR, HRV, GSR and ST features are fused together. The feature templates made up of features from the different bioelectrical signals and the context awareness template are expected to increase the information discrepancy between subjects

to improve the classification result. Therefore, each of the feature and context awareness templates from active, non-active and combination of active and non-active are fused together to create an algorithm.

A multi-algorithm approach is implemented by using the three algorithms of active, non-active and combined algorithm. The classifier (NN-FF) used for the algorithm is the same as the previous section. The classification of the active and Non-active algorithms is carried out over different networks sizes using the time frame of 3 seconds. The two segments in addition to the combined activity forms the premises for multi-algorithm implementation of the authentication system.

5.5.2 Performance of Active Algorithm

Figure 5.10 illustrates the result of the Active Algorithm classification using different network sizes. It shows the network with 70 neurons having the best result with EER of 2.5%. Following the finding in section 5.3.1, it will be noted that the active classification results followed the same pattern of the all activities. The closest to the best is the neighbouring network size with 70 neurons. The individual performance is expected to follow the same pattern therefore, using only the best network size for user authentication will be most ideal.

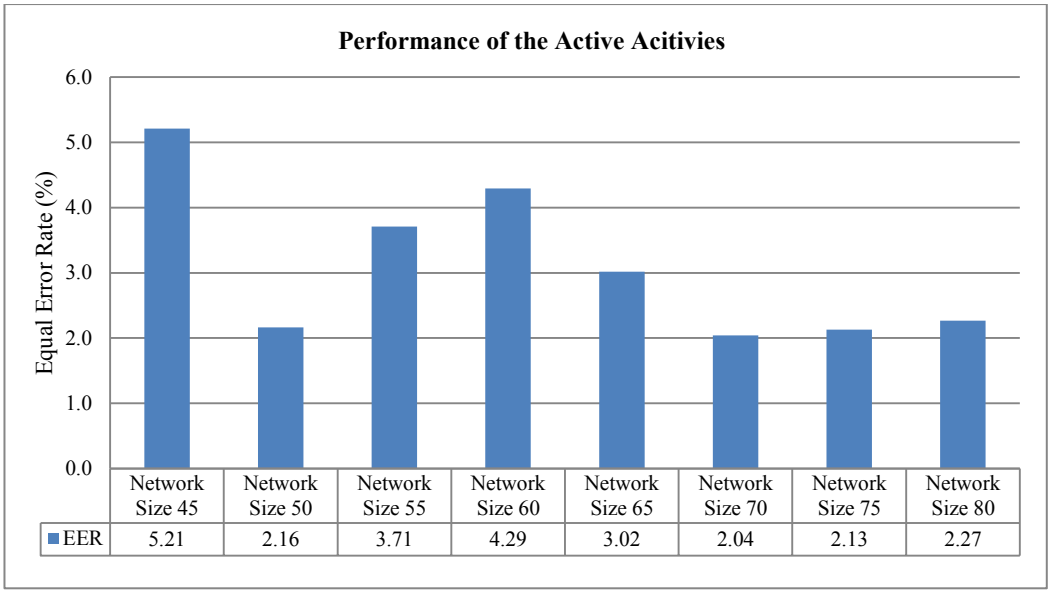


Figure 5. 10: showing the Performance of the Active algorithm

The performance of individual subject for the active algorithm classification as illustrated in Figure 5. 11 shows subject 17 and 18 as the best. The worse is scored by subject 1 with an EER of 12.56% followed by subject 10 with 9.96%. The classification with an overall performance of 2.04% EER shows 76.7% scoring below EER of 2.04%. This result performed better than the all activity classification.

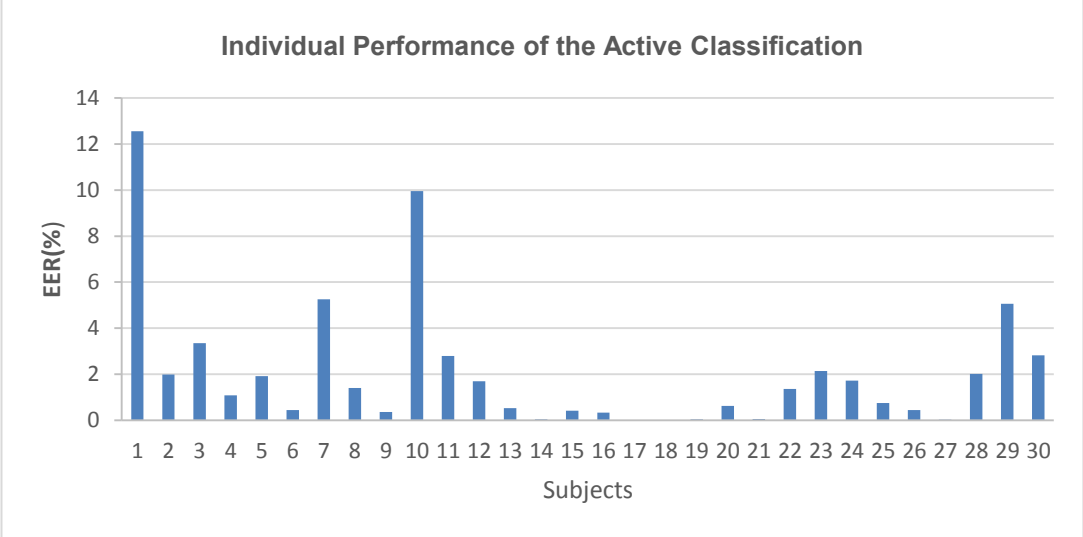


Figure 5. 11: Optimal result for each subject from the Active Algorithm

5.5.3 Performance of Non-Active Algorithm

The non-active algorithm classification accurately classified the subject to a more reasonable degree compared to the last two classifications. Figure 5.12 illustrate the best network size as 65 with EER of 0.27% with the individual performance in illustrate in Figure 5.13. Most of the result in the classification performed below 1% error rate. This result will enhance a multi-algorithm approach with most subject been in the region close or below 1% of EER.

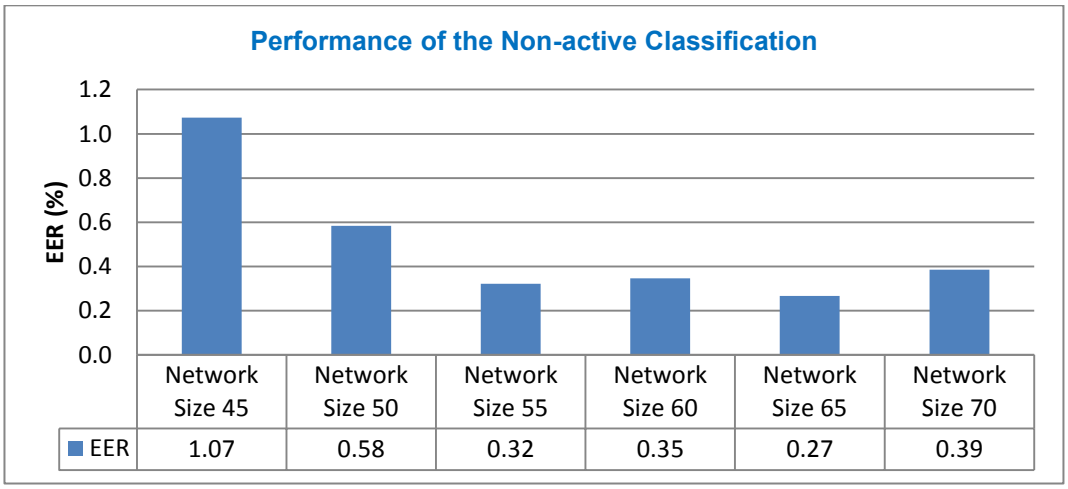


Figure 5. 12: Showing Individual Performance of the Non-active algorithm.

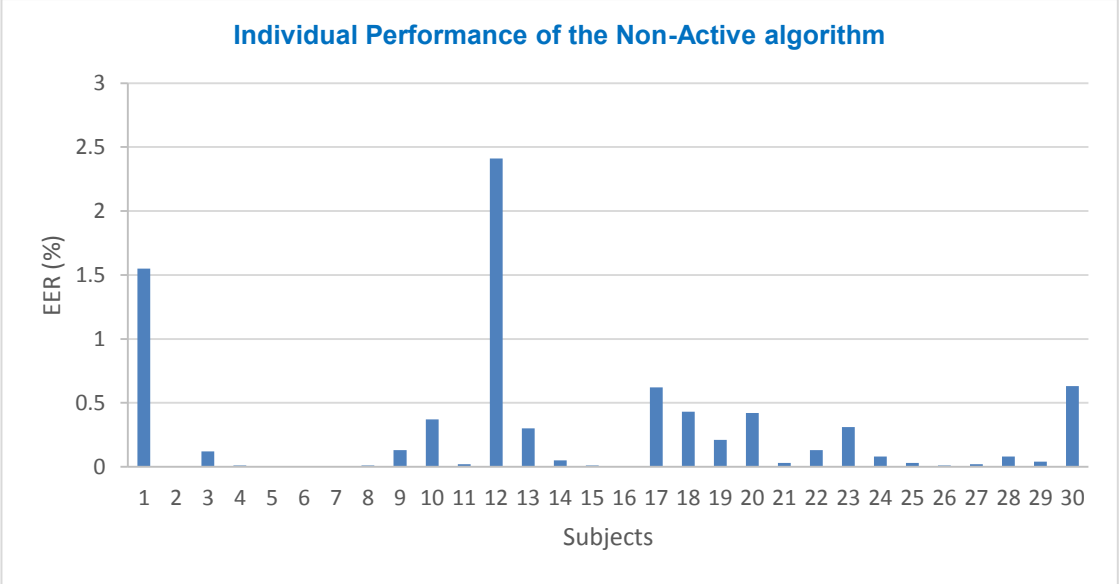


Figure 5. 13: Optimal result of individual subjects from the Non-active in EER

The individual analysis further authenticates the fact stated as only two subjects scored above 1%. Subject 1 and 12 scored EER of 1.55% and 2.41 respectively. The four subjects, 2, 5, 6 and 7 have the best results scoring 0% and 70% of the subjects scoring about the 0.27% EER of the classification result. On the bases of the above result, the use of non-active algorithm accurately discriminates the subjects compared to the combine and active algorithm. However, the use of multi-algorithm provides the ability of an authentication system to rely on more than one biometric template. The use of multiple biometric templates provides an option for optimization of the system to effectively and accurately discriminate subjects.

5.5.4 Performance of the Multi-Algorithm

In the previous section, we confined our scrutiny to the analysis of each activity segment of the bioelectrical signals. The analysis from the results of the classification of the active and non-active algorithm shows evidence of increased performance over the combined algorithm. The findings of the analysis provide potential utilization of the subject's activity

for multiple algorithms authentication system. The improved performance may not be possible using only the fusion of bioelectrical signals for classification. Therefore, the three algorithms are utilized for establishing a reliable multi-algorithm bioelectrical user authentication system. Figure 5.14, 5.15 and Table 5.10 illustrates the combine performance of the three algorithms.

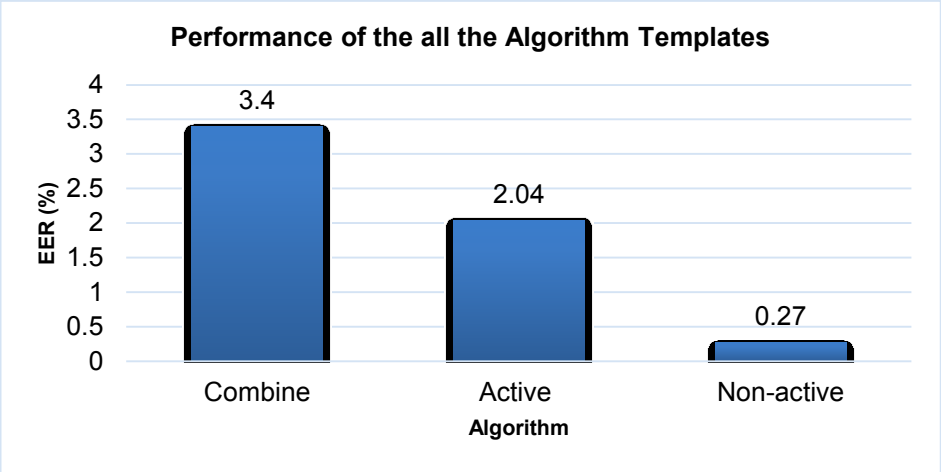


Figure 5. 14: Showing the performance of the all the algorithm templates

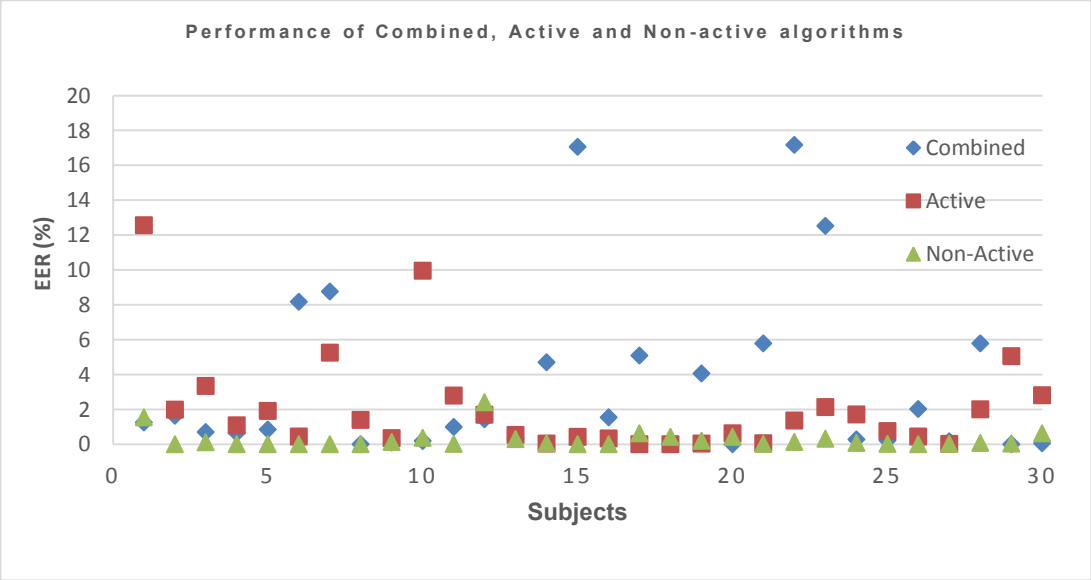


Figure 5. 15: Combine performances of the three algorithms. High: Active, Low: Non-Active and All: Combined.

Table 5.10: Performance of Combined, Active and Non-active algorithms in details

Performance of Combined, Active and Non-active algorithms											
User	Combined	Active	Non-Active	**User**	Combined	Active	Non-Active	**User**	Combined	Active	Non-Active
1	1.25	12.56	1.55	**11**	1.00	2.79	0.02	**21**	5.79	0.05	0.03
2	1.63	1.99	0.00	**12**	1.44	1.70	2.41	**22**	17.17	1.36	0.13
3	0.70	3.35	0.12	**13**	0.33	0.53	0.30	**23**	12.52	2.14	0.31
4	0.64	1.08	0.01	**14**	4.71	0.04	0.05	**24**	0.28	1.72	0.08
5	0.84	1.91	0.00	**15**	17.07	0.42	0.01	**25**	0.22	0.75	0.03
6	8.17	0.44	0.00	**16**	1.55	0.33	0.00	**26**	2.02	0.44	0.01
7	8.76	5.25	0.00	**17**	5.09	0.00	0.62	**27**	0.17	0.03	0.02
8	0.01	1.40	0.01	**18**	0.01	0.00	0.43	**28**	5.79	2.01	0.08
9	0.09	0.36	0.13	**19**	4.06	0.04	0.21	**29**	0.01	5.06	0.04
10	0.18	9.96	0.37	**20**	0.01	0.63	0.42	**30**	0.06	2.82	0.63

In user authentication, different algorithm complements each other by using different inputs from the biometric sample (Clarke, 2011a). The used of multi-algorithm ensures that a subject is accurately authenticated as the person they claim to be. It also increases guarantee of the system by increasing the trust of authenticity (Lim et al., 2017). Besides sustaining the trust of the system, the system should able to authenticate the subject irrespective of the action or activity the subject is engaged in during the authentication period. Comparing the results from the three algorithms, the worst score is from subject 22 (combine algorithm) with an EER of 17.17%. The combination shows great deal of strength of the multi-algorithm approach with only 4 subjects scoring above 10% EER making it about 13% of the subjects. It is interesting to note that only one subject from the active algorithm scored above EERR of 10% while the three remaining are from the combine algorithm. Subject 1 scored 12.56% EER from the active algorithm while subject 15, 22 and 23 scored 17.07%, 17.17% and 12.52% respectively from the combine algorithm. Analysis from previous studies using Wavelet Transform for feature extraction or Neural Network for classification of bioelectrical signals as illustrated in Table 5.11 are all done using success rate. The best performance using Neural Network for classification

is 99.09% while the worse is 78.6%. The best result using wavelet transform for feature extraction is 95% while the worse have 89%. That puts the performance of the system's accuracy at between 95% - 99.09%.

Table 5.11: Summary of result using either Neural Network or Wavelet Transform for classification or feature extraction of bioelectrical signals

Author/Year	Signal	Feature Extractor	Classification	Success rate
(Subasi, 2007)	EEG	Wavelet Transform	Neural Networks	93.2%
(Chan et al., 2008)	ECG	Wavelet Transform	Correlation Coefficient (CC)	89% - 95%,
(Hema et al., 2008)	EEG	Welch Algorithm	Neural Network	97.5%
(Hema and Osman, 2010)	EEG	Power Spectral Density	Neural Network	78.6%.
(Tawfik and Kamal, 2011)	ECG	Discrete Cosine Transform	Neural Network	99.09%
(Sidek and Khalil, 2011b)	ECG	Wavelet Transform	Radian Basis Function	91%
(Sidek and Khalil, 2011b)	EEG	Wavelet Transform	Radian Basis Function	95%
(Hema and Elakkiya, 2012)	EEG	Power Spectral Density (PSD)	Neural Network	97.2%-98.85%
(Colomer Granero et al., 2016)	EEG, ECG & GSR	Independent Component Analysis	Random Forest	89.76%
(Arafat and Bellegdi, 2017)	EEG	wavelet transform & Fourier transform	TreeBoost, Random Forests, and support vector machines	97.5%
(Heri Kuswanto, 2017)	EEG	Discrete Wavelet Transform	Random Forest (RF) and Support Vector Machine (SVM),	80%

In comparison to the prior works with performance metrics using success rate, there is the need to compare the research work with the prior work in success rate. The success rate is either equal to or greater than (1-EER) (Al-Rubaie and Chang, 2016). Therefore, to convert EER to success rate this following equation is used:

$$Success\ Rate = 1 - (\frac{EER}{Number\ of\ subjects})\ X\ 100$$

Equation 5.1: Calculation of success rate

Using the equation, the success rate for the performance of the three algorithms is calculated as:

The combine algorithm,

$$Combine\ algorithm\ Success\ Rate = 1 - (\ \frac{3.4}{30}\ )\ X\ 100 = 88.67\%$$

The active algorithm,

$$Combine\ algorithm\ Success\ Rate = 1 - \left(\frac{2.04}{30}\right) X\ 100 = 93.2\%$$

The non-active algorithm,

$$Combine\ algorithm\ Success\ Rate = 1 - \left(\frac{0.27}{30}\right) X\ 100 = 99.1\%$$

Using the success rate, the algorithms achieved a high performed with the non-active algorithm performing better than the best result from the prior works in Table 5.11. In addition to their performance, they are all intrusive making the methods not convenience with a usability issue.

5.6 Discussion

To achieve the desired result, the experimental work exploited different approach by optimizing both different time frames and classifiers successfully to discriminate the subjects. The use of more than one bioelectrical signal improved the EER compared to the fusion of the different levels of the sub-band decomposition of the bioelectrical signal of the heart rate in experiment two. This is also seen with the fusion of the bioelectrical signals of ST and GSR features which significantly improve the EER compared to unimodal of the heart rate features. This is also the same for the speed and altitude feature fusion classification result. The fusion of all bioelectrical signals enhanced the entire result of the classification. The possible reason for this improvement is the fact that the different signals contain different discriminatory information. Not all fusion affects the output positively; some can affect the result negatively. Some information may contain either

positive, negative or no discriminative information therefore affecting the result positively or negatively (Clarke 2014).

The use of bioelectrical signals for the research work has its advantage compare to other biometrics. While bioelectrical signal is always present in a subject, there might be a failure to acquire one signal or more during data collection. This can reduce the amount of information present at any time. To overcome this, multi-dimensional vector can be relied upon to improve the usability as well as the security. For example the extraction of one bioelectrical signal with three algorithms created from it enhances its application for security because more information is extracted. To improve on authentication system, the use of different stratagem like using multi-classifier, dynamic feature selection, multi-algorithm is expected to achieve a better result. Therefore, employing multi-algorithm approach to overcome the issue face with using a signal bioelectrical signal as earlier discussed in the work is eliminated. To improve on the system performance is to increase the rate at which a genuine subject accesses the system. The implementation of the proposed multi-algorithm approach will enhance the system but using the same threshold for all algorithms might be counterproductive. Therefore, adjusting the threshold based on each algorithm performance will maximise performance. Usability is essential in user authentication implementation therefore; it is taken into consideration in the design of the system. While it should be noted that security is the focus in an authentication system, usability is also desirable. The use of bioelectrical signal and the contextual information were useful for creating a template to successfully classify a subject. While this has proven to be effective, however there is the likelihood of an impostor gaining access while a genuine subject is rejected by the system. To increase the acceptance rate of genuine subjects while rejecting impostor, the algorithms will be implemented using the most suitable algorithm in authenticating a subject. Table 5.12 illustrates the division of the

result into 5 segments for easy analysis of the performance. The combine algorithm has 63.3% of the subjects scores 0 – 2% while this is followed in percentage by the scores of 4 – 6% with 16.7%. The combine algorithm has 19 subjects scoring below EER of 2%. This shows the best performance have more subjects but is not followed by the next score range of 2 – 4% in term of number of subjects with 5 subjects.

Table 5. 12: The three Algorithm scores and the number of subject within a certain score range

Threshold in EER (%)	Algorithms		
	Combine	Active	Non-Active
0 – 2	19	21	29
2 – 4	1	5	1
4– 6	5	2	0
6 – 8	0	0	0
8– 10	2	1	0
10 - above	3	1	0

$$Performance\ (\%)\ = \frac{\text{Total Number in each threhold}}{Number\ of\ subjects}\ X\ 100$$

Equation 5.2: Calculation of the performance in percentage

The active algorithm has 70% scores of 0% – 2% while the non-active algorithm has 96.7% of scores 0% – 2%. This is followed by the score of 2.1% – 4% unlike the combine algorithm with 5 subjects and 1 subject for the active and non-active algorithm respectively. The combine algorithm scores on the 0% – 2 % threshold might be attributed to the fact that while the active and the non-active algorithm use feature with no 'zero' feature value, the combine has much of it in the section where the subject is not active. The non-active algorithm did not include steps information for the context awareness template because while the subject is non-active, the steps are not recorded. The active algorithm includes the steps because values are recorded while in action. The combine algorithm is the same as the original signal with the steps context awareness included. The steps as

earlier stated records the values when active and no values when non-active but during the feature extraction, the values are used irrespective of the motion action. The three algorithms performance is used to analysis the general performance of the system by setting a threshold from 2 – 10% with an increment of 2%. With a good degree of performance from the 0 – 2% region, it will be expected that the result will be ideal for a user authentication system but in as much as security is a concern usability should also play a role in the design of the authentication mechanism. The best algorithm for user authentication is the not-active algorithm; this is when the subjects are non-active. This may be due to the stability of the subject's bioelectrical signals when at rest (non-active period). In the daily use of mobile device, most subjects utilized their application mostly when in non-active position like sitting, standing, lying down than when the subject is active like walking, running etc. This position supports the anticipation that the system will be more effective because there will be more non-active authentication, this is an advantage to the system. The system is expected to use the most appropriate algorithm to authenticate a subject. The possibility of an alternate algorithm suitable for authenticating a subject is based on the activity the subject is engaged in. The decision will be based on the template that contain similar characteristic that can be used to discriminate the subject. The combine algorithm contains similar characteristic of both the active and not active algorithm. Therefore if the active or the non-active is not capable to authenticate a user then the combine will be used to authenticate the subject. There are many factors that can be employed to make authentication decisions by the intelligent decision component of the system. This includes the type of action the subject is engaged when the signals are extracted. The subject could be idle or in motion at the time of extraction, this could be sub-divided in the type of motion or idleness. The idle could be sitting, standing, lying down or the subject could even be in a moving vehicle. A subject could be active when the

signal is extracted but the motion type could be walking, jogging, running or even jumping (skipping). It could be difficult to decide but with the application of intelligent decision by the system, the motion type could be obtained for an accurate discrimination of the subject. To achieve an optimal authentication result for the system, it will reasonable to use the 2% EER as the highest level of the security level. To evaluate the performance of the multi-algorithm, the subject performance within the 0 – 2% EER bracket is used in order to achieve a good discrimination of the subjects as illustrated in Table 5. 13.

Table 5. 5: Comparison of the Multi-Algorithm using threshold between 0-2% EER

Security level using threshold of 0 – 2%			
Threshold	**Combined**	**Active**	**Non-Active**
0 – 0.4	11	8	24
0.41 - 0.8	2	6	4
0.81 - 1.2	2	1	0
1.21 - 1.6	3	2	1
1.61 – 2.0	1	4	0
Total	19	11	29

5.7 Conclusion

The use of a single bioelectrical signal could discriminate subjects however, it is not sufficient. The application of fusion of features from multiple bioelectrical signals has shown to have improved the discrimination of subjects. The use of the best time frame further improved the system. The best time frame is applied to different networks with different neuron sizes with the aim of attaining optimal performance of the system. The optimal performance achieved an impressive result with the fusion of all bioelectrical signals and contextual information irrespective of activity. By using the best time-frame and network size, it achieved an Equal Error Rate of 3.40%. To deploy a more flexible system to improve on the earlier result, a multi-algorithm is considered. It will be

appropriate to accept all genuine subjects while rejecting impostors. Therefore, an approach is exploited by dividing the signal into categories depending on the subject's activity during the extraction. The ability for the authentication system to successfully authenticate a subject irrespective of what the subject is doing should be crucial. The use of a subject's activity to categorise the signal into different algorithms improved the classification. The different algorithm's individual performance showed better result with many subjects achieving an EER of 0%. The study established the fact that the use of more than one algorithm improves the entire result of the system.

The advantage of this approach is that it solves some limitation faced by some biometric system. For example, gait authentication cannot authenticate a subject when the subject is idle but with bioelectrical signals there is always discriminatory information irrespective of the state the subject. The subject will not be involved in the authentication process that makes it non-intrusive and convenient for the subject. The application of data fusion at the pre-classification level is to reduce the power consumed during classification. This is because classification of each signal feature set separately will increase the system power consumption.

6. Design and Development of a Novel Bioelectrical Body Recognition (BEBR) System

The previous chapter have established the premise for a user authentication system employing fusion of the bioelectrical signals and context aware data. To implement a secured user authentication system, there is the need to consider some factors discussed in the previous chapter in order to overcome them. The issues include:

- Intrusiveness in the user authentication system as presently implemented brings about usability issues.
- Improving upon the authentication security mechanism to reduce the false rejection of genuine subjects and false acceptance of impostors to access the device

To overcome the issues raised above with the aim of the architecture is to increase the security level beyond that presently offered by designing a framework that will extract the required data transparently and propose a novel decision process to increase the rate of acceptance of genuine subjects while rejecting impostors.

6.1 A Novel Bioelectrical Body Recognition (BEBR) System

To provide a reliable and secure user authentication system for a mobile device like smart phone, a novel bioelectrical body recognition (BEBR) framework is proposed. The novel bioelectrical body recognition framework verifies a subject based on bioelectrical signals and contextual information extracted with a wearable device (smart watch) and a mobile device (mobile phone) from the subject. The bioelectrical signal and the contextual information extracted are divided into two based on the subject's activity. The original data and the divided data are based on the subject's activity in motion or idle at the time of extraction. The three set of data are identifies as combined, active and non-active signal and its contextual data. The bioelectrical signals and its contextual information is

effectively utilised by fusing both data together. During the time to acquire, the mobile phone will use the inherent authentication system of the device till it is replaced with the BEBR authentication mechanism dependence on extracting enough bioelectrical signals over a specified minimum duration. The framework is designed to indicate its readiness for implementation when the amount of information need to activate the proposed user authentication framework is achieved. After attaining the required data needed, a request is made for the subject to answer some knowledge base questions, this is used to reactivate the system whenever it fails to authenticate a genuine subject due to issues like ill health that affect bioelectrical signals (Jones et al., 2008). When the request granted, the mobile device adapts the BEBR authentication mechanism. After activating the BEBR authentication mechanism, mobile device is automated depending on the setting of time frame to be used by the subject for re-authentication depending on the authentication requirement of the mobile phone. The data is extracted periodically with the activation of the mechanism. With the full implementation of the BEBR, the mobile device authenticates the subject at the start-up of the phone to access the services of the phone and this done continuously as long as the subject (smart watch) is within the communication distance of the mobile phone but in a situation where the phone is disconnected due to the subject walking away from the communication range of the phone it will disconnect and re-connects when the subject is back within the range.

6.2 BEBR Framework

The proposed bioelectrical body recognition system as illustrated in Figure 6.1 is designed to extract multiple bioelectrical signals and context awareness data for a multi-algorithm user authentication implementation.

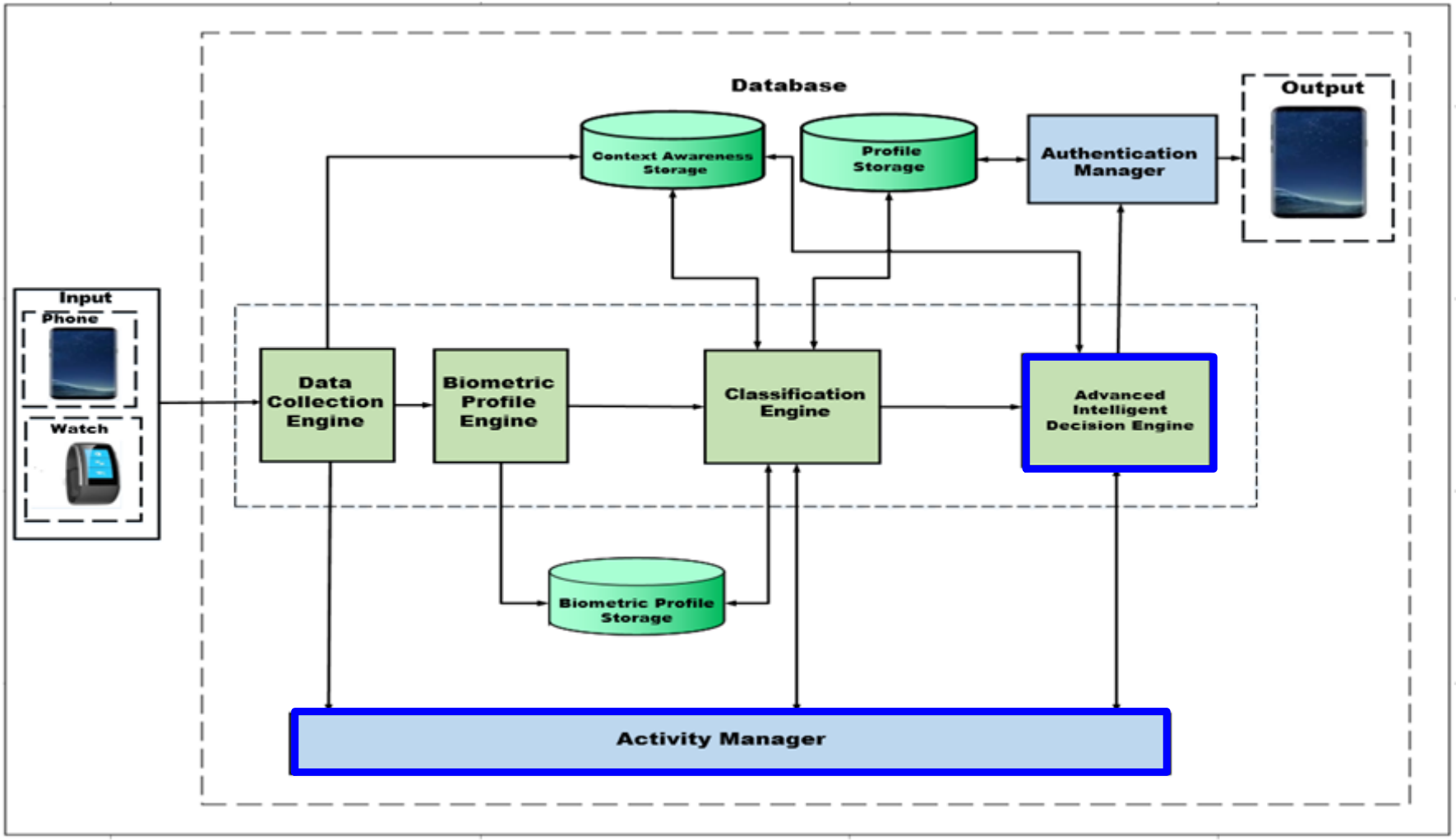


Figure 6. 1: A Novel Bioelectrical Body Recognition Framework showing the added layers with blue borders

The BEBR framework designed is based upon research by a wider body of work carried out within the Centre for Security, Communication and Network (CSCAN) of the University of Plymouth . The proposed framework adopted some engine processes from works by Clarke (Clarke 2007), Li (Li, 2012) and Saevanee (Saevanee et al., 2015), built upon it to improve the architectural structure of the proposed BEBR framework. The framework in Figure 6.1 shows the portion with thick blue border (AIDE engine and Activity Manager) as the layers contributed by this work to the framework from others within CSCAN. The proposed architecture has been attained by employing combination of engines, managers and components with the body recognition framework. The engine includes the Data Collection Engine, Biometric Profile Engine, Classification Engine and Advance Intelligent Decision Engine while the managers include the authentication and activity manager. Another important component is the database. The database consists of context awareness storage, profile storage and the biometric profile storage. These engines, managers and database carry out specific task with the help of the different components which shall be discussed in detail.

In a brief description of the framework process, the different engines process the data extracted by the smart watch and smart phone. The smart watch extract both bioelectrical signals and contextual information while the smart phone extracts only contextual information in the proposal. The smart watch uses a custom-built application within the smart watch to extract and transmit the extracted data. At the receiving end, the data collection engine on the smart phone receives the transmitted data and pre-processes the received data by dividing the data into two categories base on subject's motion activities at the time of extraction. The two categories are the active and non-active. The original data from where the active and non-active data is extracted from is used as the combined active data.

The biometric profile engine segments the three categories of the combined, active and non-active data. Each of the data categories are segmented into fixed segments using time frame.

The feature extraction engine extracts the features form only the bioelectrical signals from each of the time frame segments in each data categories. The contextual information is later fused with bioelectrical signal feature into a biometric profile template. The biometric profile engine general biometric algorithms for classification form the feature profile templates. The Classification Engine classifies the subject using the most suitable algorithm. The most suitable algorithm is selected based on the activity associated with the segment using information provided by the activity manager. The classification result is sent to the advance intelligent decision engine that in turn verifies the subject base on the intelligent information from the contextual data and the activity manager. The advance intelligent decision engine verification enhances the classification output by providing more information on the subject from contextual data. The contextual data includes but not limited to the Global Positioning System (GPS), schedule information on calendar appointments, motion information etc. The AIDE used the contextual information to evaluate the subject after classification by appending values to each of the context awareness information extracted that is associated with the template time of extraction. The decision to accept or reject the subject is taken by the authentication manager based on the information from the advance intelligent decision engine. The input data is collected through devices, which in this case are the mobile phone and the smart watch. The data input device and the different engines; managers and components that made up the authentication framework will be further discussed in detail.

6.2.1 Input Device

To overcome the issue of usability and to be flexible in term of input device, any wearable device that can extract the required information (bioelectrical signals and contextual information) and able to communicate with a mobile device could be used as input devices. This will maximise its deployment for user authentication using any wearable and mobile devices that can communicate with each other and with available sensors to extract the

required data. Therefore, the framework utilises a wearable device taking advantage of the variety of bioelectrical signals and contextual information that can be extracted via Bluetooth connection to a mobile device. The wearable and the mobile device are deployed as data input device depend on the ability to extract the required data. To overcome intrusiveness that is one of the goals of the framework, both devices can extract the data without the intervention of the subject. This will eliminate memorability of inputting credentials as stated earlier. The output and input devices are automated to request for data sample and to extract and present the data sample respectively thereby making the process transparent to the subject. The implementation of a non-intrusive biometric data extraction will improve upon transparent user authentication system as presently practiced.

6.2.2 Data Collection Engine

The data collection engine is domicile on the smart phone while the smart watch is fitted with custom data controller that segments the different bioelectrical signal extracted by the different sensors installed on it. The custom controller in the smart watch collate the data and transmit to the phone. This enables the bioelectrical signals, contextual information and time stamp etc. to be stored in a table form as illustrated in Figure 4. 6: Data file extracted using Microsoft band. The communication channel is via a Bluetooth between the smart watch and smart phone. The data collection engine as illustrated in Figure 6.2 is automated to extract the data, segment the data based on the activities. The data collection component is activated once the phone established connection with smart watch. The process is activated on the background of the device operating system (OS) as long as both devices can communicate. The storage of the data table format depends on the OS of the mobile phone. The application in this case provided an option for selecting the data table file format. This is important as the data storage components are expected to use the same file format for processing the data it receives. The data is collected synchronously and logged as a table with the detail

information of the bioelectrical signals, context awareness data, activity (motion) type, time and date of extraction etc.

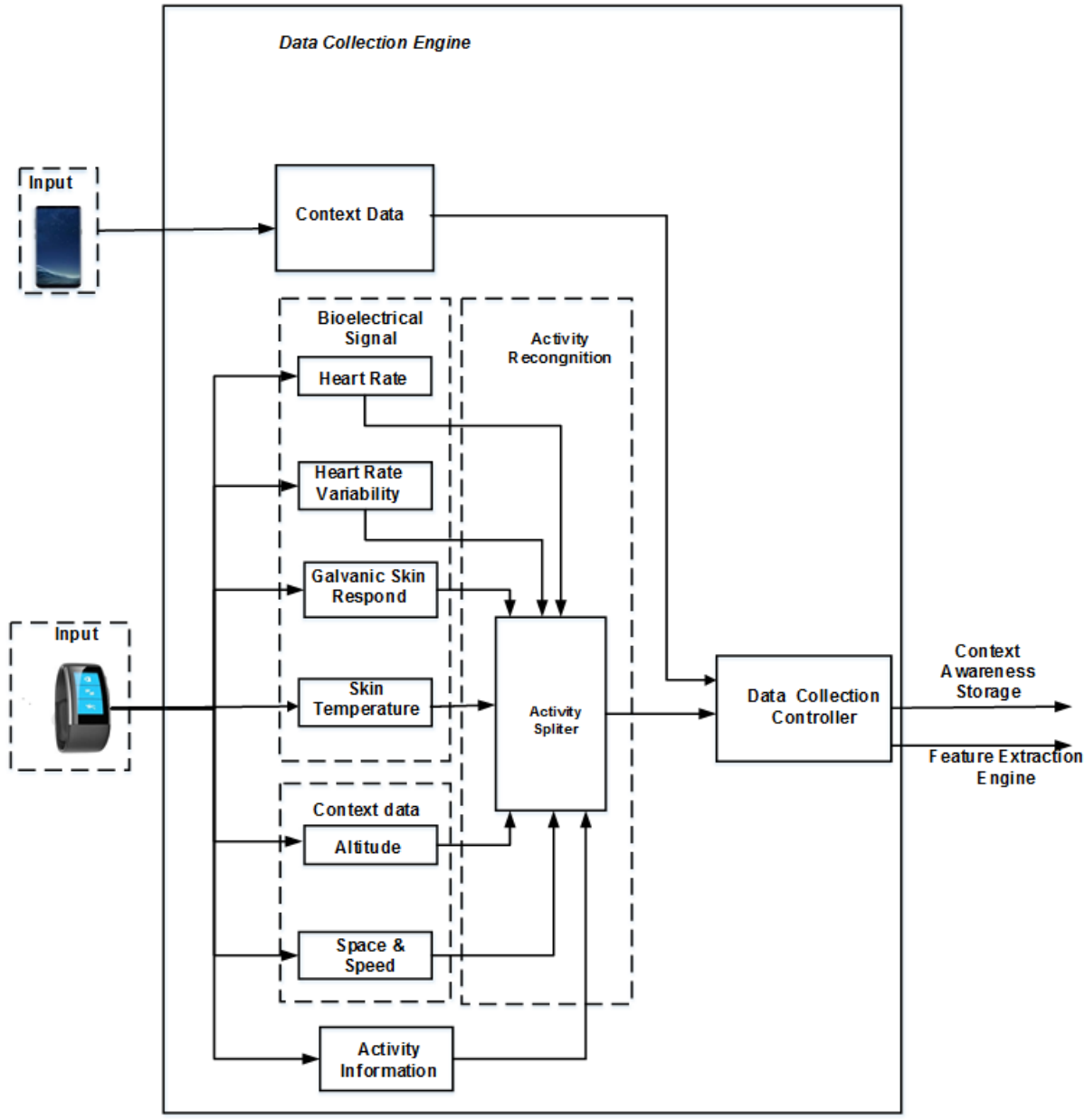


Figure 6. 2: Data Collection Engine

When the subject is not in motion, irrespective of the action e.g. lying down, standing or sitting, the system identify it as idle therefore, it logs and assign a numeric value in the activity identification table as illustrated in Table 6.1 but when in motion, it could be fast or slow like walking and running different identification is given to the different type of motion.

Table 6. 1: Activity Identification Table

Date	Time	Activity ID	Activity Type
4/04//2018	12:40	1	Idle
4/04//2018	12:41	2	Waking
4/04//2018	12:43	2	Walking
4/04//2018	12:44	3	Jogging
4/04//2018	12:45	3	Jogging
4/04//2018	12:46	4	Running
:	:	:	:

The main function of the activity splitter is to provide information for the data collection engine on the activity the subject is engage in during extraction. This is done by the activity splitter segmenting the time of any activity into the motion type and every data associated with the time is logged into the appropriate table assigned to it on the activity identification table. The activity identification table is used for segmentation of the data when a new bioelectrical signal or contextual data is extracted. Every data with '1' is segmented as a non-active data while any identification higher than '1' is logged as active data. The third logs all the data irrespective of the identity as combine data. The contextual information from the smart phone is stored on a different table. This is because when the bioelectrical signal and the contextual information are extracted, the phone contextual information is simultaneously extracted therefore, it will be better to use a different table to store the information separately. The contextual information from the phone is stored on the context awareness table as illustrates in Table 6.2. The contextual information stored on the table includes the GPS information, schedule information on calendar appointments, phone orientation, typing style, steps etc. The context awareness table gives information on the availability or non-availability of the needed context awareness information at the time the information is extracted. When available it is access to from the information location for used by the appropriate engine.

Table 6. 2: Context Awareness Table

ID		1	2	3	4	5	6
Date	Time	GPS	Phone touchscreen/ orientation	SMS/Calendar	Typing style	browsing pattern	Steps
20/02/18	10:26	Yes	Nil	Nil	Yes	Yes	Yes
20/02/18	10:28	Yes	Yes	Nil	Yes	Yes	Yes
20/02/18	10:28	Yes	Yes	Nil	Yes	Nil	Nil
20/02/18	10:23	Yes	Yes	Nil	Nil	Nil	Nil
20/02/18	10:01	Yes	Yes	Nil	Nil	Yes	Yes
20/02/18	10:26	Yes	Yes	Yes	Yes	Yes	Yes
:	:	Yes	Yes	Yes	Yes	Yes	Yes

The bioelectrical signal and contextual information from the smart watch are stored in a temporary data table as demonstrated in Tables 6.3, 6.4 and 6.5. The table can be automated to accept only the data that is needed by activation a box provided as illustrated in Figure 6.3

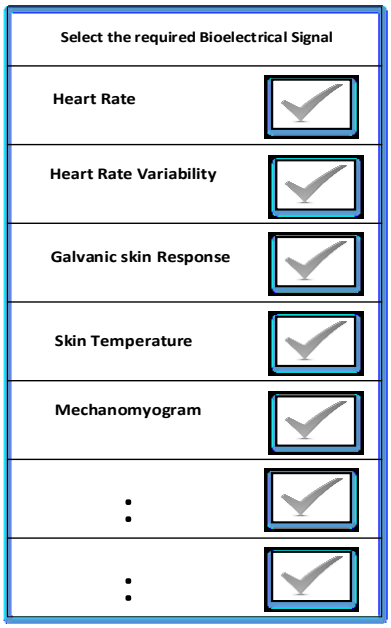


Figure 6. 3: Bioelectrical activation box

The minimum requirement for the BEBR authentication mechanism to be activated is extracting 3600 seconds worth of data. The 3600 seconds worth of data is expected to be attained for each of the different activity tables. Therefore, any table that has not attained the required amount of logged information cannot be used by the system at the initial period in the authentication process. For the table to be sent for feature extraction at the first instance, each of the three tables should meet the minimum requirement. Therefore, even if two tables meet the requirement of feature extracted and templates created, the system will wait for the last table to meet the requirement before that system is activated.

Table 6. 3: The Temporary Data Table for Combined Activity

Date/Time	Activity ID	Bioelectrical Signal				Context Awareness				Temporary Storage
		Heart beat		Body Temperature		Momentum		Altitude		
		HR	HRV	GSR	Skin Temp.	Speed	Pace	Altitude Ascended	Altitude Descended	
04/04/2018/12:40	1	66	0.91256	1608	29.08	0	0	81650	77880	\\dataprofile\combined
04/04/2018/12:40	1	66	0.91256	1608	29.08	0	0	81650	77880	\\dataprofile\ combined
04/04/2018/12:46	2	70	0.879376	2252	29.43	952	105	82866	78662	\\dataprofile\ combined
04/04/2018/12:46	2	70	0.879376	2252	29.43	952	105	81650	77880	\\dataprofile\ combined
04/04/2018/13:02	3	89	0.1045674	45000	29.57	1073	122	82914	78708	\\dataprofile\ combined
04/04/2018/13:02	1	65	0.91256	1600	28.06	0	0	81650	78708	\\dataprofile\ combined
:		**:**	**:**	**:**	**:**	**:**	**:**	:	:	:

Table 6. 4: The Temporary Data Table for Non-Active Activity

Date/Time	Activity ID	Bioelectrical Signal				Context Awareness data				Temporary Storage
		Heart beat		Body Temperature		Momentum		Altitude		
		HR	HRV	GSR	ST	Speed	Pace	Altitude Ascended	Altitude Descended	
04/04/2018/12:40	1	66	0.91256	1608	29.08	0	0	81650	77880	\\dataprofile\non-active
04/04/2018/12:40	1	66	0.91256	1608	29.08	0	0	81650	77880	\dataprofile\non-active
04/04/2018/12:40	1	67	0.91286	1608	29.08	0	0	81650	77880	\dataprofile\non-active
04/04/2018/12:40	1	67	0.91286	1608	29.08	0	0	81650	77880	\\dataprofile\non-active
:		:	:	:	:	:	:	:	:	:

Table 6. 5: The Temporary Data Table for Active Activity

Date/Time	Activity ID	Bioelectrical Signal				Context Awareness data				Temporary Storage
		Heart beat		Body Temperature		Momentum		Altitude		
		HR	HRV	GSR	ST	Speed	Pace	Altitude Ascended	Altitude Descended	
04/04/2018/12:46	2	70	0.879376	2252	29.43	952	105	82866	78662	\\dataprofile\active

04/04/2018/12:46	2	70	0.879376	2252	29.43	952	105	81650	77880	\\dataprofile\active
04/04/2018/13:02	3	89	0.1045674	45000	29.57	1073	122	82914	78708	\\dataprofile\active
04/04/2018/13:02	3	89	0.1045674	45000	29.57	1073	122	82914	78708	\\dataprofile\active
:		:	:	:	:	:	:	:	:	:

The bioelectrical signals are extracted at a rate of 8 samples per second. This brings the temporary data table to total of 288,000 data points for each of the three tables. This will be further discoursed in the feature extraction engine section. It should be noted that the disconnection between the two devices of the phone and the watch is considered. The issue faced after disconnection as discussed in Chapter 4 is considered to make sure all the data information requires on the tables are available before it is log on the table. That is, all information to be logged into the table should be extracted simultaneously with the required data (i.e. if only three of the required bioelectrical signals are extracted with one not available for certain duration, the table will only accept the duration when the four signals are present). The delay in extraction for some data is because some information like the skin temperature takes some second before it starts logging the information. The bioelectrical signals to employ for the system can be selected based on the number of signals sensor available on the smart watch for which the device can extract. The more the bioelectrical signal, the more the information for discrimination. At the installation of the system, the table is empty with provision for indicating the number of bioelectrical signals and contextual data the watch and the phone can extract and transmit. However, the architecture is designed to accept any bioelectrical signal from any wearable device if it meets the International Standard Organisation (IOS) requirement. After the data are collected, the pre-processing of the bioelectrical signals is basically the same process across the extracted signals. The pre-processing involves dividing the signals into three divisions of combined, active and non-active bioelectrical signals.

- **Activity Splitting component**

The splitting of the bioelectrical signals into an appropriate category is done by an activity splitting component. Every information log into the data file is associated with a time stamp and motion activity information see Table 6. 1: Activity Identification Table. The activity splitting component in data collection engine use the motion activity identity to divide the data extracted. The active signals include walking, jogging and running while a non-active signal indicated as Idle includes standing, sitting, lying down. The active and non-active data with the combined data (original) form the three data for every signal and context awareness data extracted. For example, the HR signal is sub-divided into active heart rata signal, non-active heart rate signal with the combined signal (the extracted HR rate signal). This is done for all the bioelectrical signals and contextual data. The data collection engine transmitted the sub-divided data to the feature extraction engine. From the extraction of the data by the sensors in the watch to the transmission of the data to the phone, the procedure is seamless. The data collection engine is domicile on the phone that automatically stores all processed data on the temporary data table as stated earlier. In this experiment, a third-party application also domicile on the phone is used to automate the search for the phone continuously till it is found then connection is established. The information from the activity slitter is sent to the activity manager where the activity identification table is store.

6.2.3 Biometric Profile Engine

The biometric profile engine as illustrated in Figure 6.4 prime duty is to generate the various biometric profile templates after extraction of the feature from the signals for the classification engine. The biometric profile is divided in to two sections that include the features extraction and the biometric profile template generation.

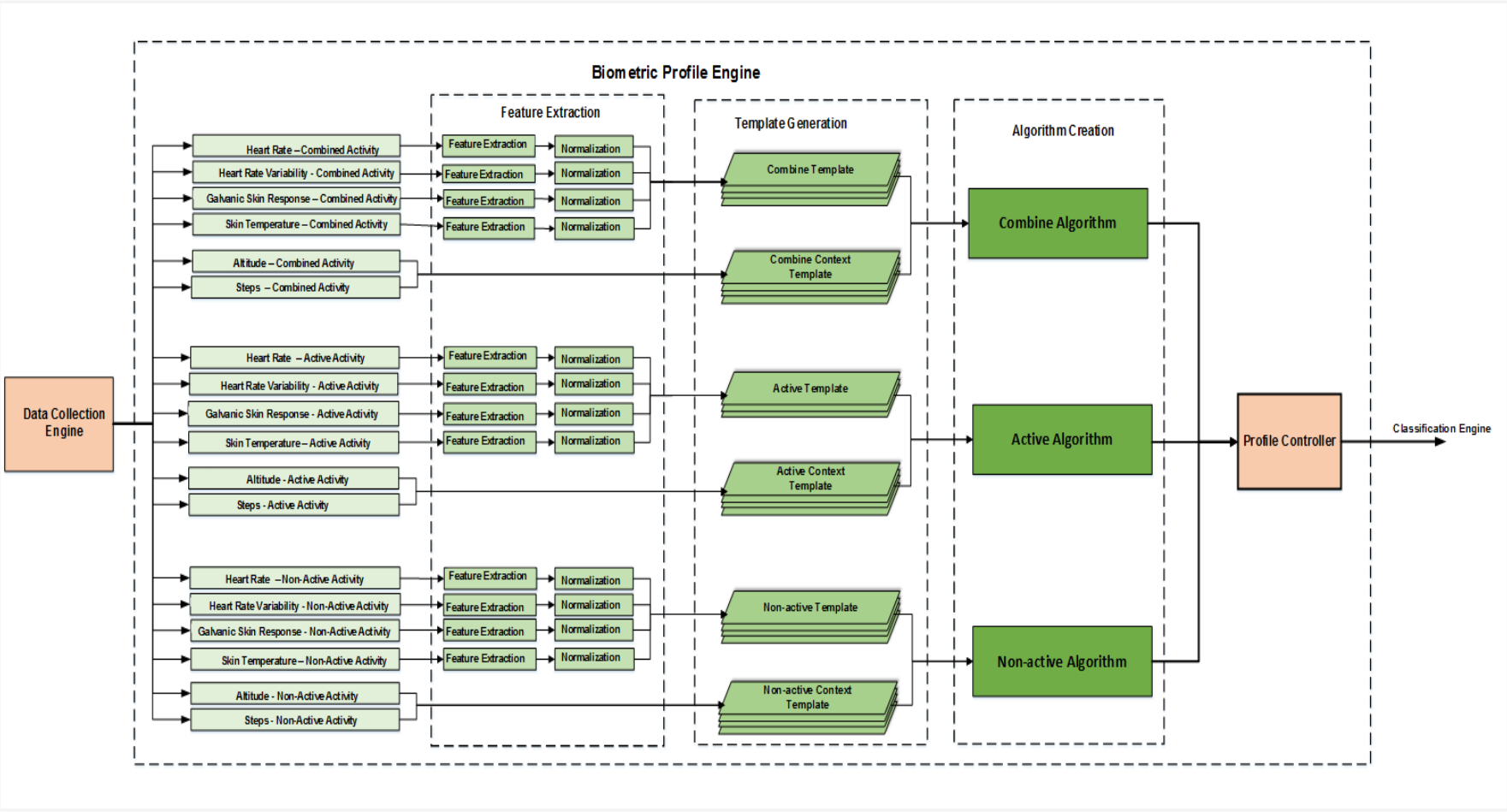


Figure 6. 4: Biometric Profile Engine

6.2.4 Feature Extraction Component

The feature extraction section of the biometric profile engine does the feature extraction. Before the features are extracted, from the three temporary data table of combined, active and non-active bioelectrical signals and contextual data, the data collection engine are segment the signal into specified authentication windows. The bioelectrical signals are divided into fixed authentication window of 3 seconds per frame. This creates a frame of 24 data points in every 3 seconds. From the experiment in chapter 4, one-hour worth of data is considered as sufficient. Therefore, the framework collects the minimum requirement per day over seven days to meet the minimum number of frames requirement for initial feature template creation. The maximum frames are not required on daily bases but only at the first data acquisition. (If there is no disconnection within the one hour, the combined data could meet the requirement for a day). It extracts the features from each of the bioelectrical frame while no feature is extracted from the contextual information as they remain in their original state.

Table 6. 6: showing Temporary data table

Data ID	Data Type	Class Name	Data Name
1	Bioelectrical Signal	Heart beat	Heart Rate
2	Bioelectrical Signal	Heart beat	Heart Rate Variability
3	Bioelectrical Signal	Body Temperature	Galvanic Skin Response
4	Bioelectrical Signal	Body Temperature	Skin Temperature
5	Context Awareness	Steps	Speed
6	Context Awareness	Steps	Pace
7	Context Awareness	Altitude	Altitude Ascended
8	Context Awareness	Altitude	Altitude Descended
:	:	:	:

The extraction of features from the bioelectrical signals in each of the data table is processed depending on the feature extraction technique as described in chapter 5 see Figure 6. 2: Data

Collection Engine. The class name of the data as illustrated in Table 6.6 is used to apply the feature extraction technique for each signal. The heart beat dataset used discreet wavelet transform extraction technique while the body temperature dataset used the wavelet packet entropy for its feature extraction. The biorthogonal wavelet extracted 10 statistical features from each of the heart beat dataset while 6 features are extracted from each of the body temperature dataset. The extracted feature vectors are normalised between 0 and 1 before fusing the entire bioelectrical signal feature vectors into a single feature template. The bioelectrical signal feature (fused) template and the context awareness template are fused to create a unified feature template for each subject. The unified biometric profile templates are forwarded to the classification engine by the feature extraction controller.

6.2.4.1 Context Awareness Data

The quality of a feature temple for user authentication should have much information to discriminate a subject from others (Abboud and Jassim, 2012). Therefore, to increase the information available within the feature vector space, context awareness is employed. The contextual information includes the subject's steps which is denoted by the pace and speed extracted during walking, jogging and running using a speedometer sensor. The other contextual information extracted is the altitude information from the degree of ascending and descending using an altimeter sensor. The altitude information is employed for the three categories, but steps are utilised for only the active and the combine activities algorithms. This is because the steps are not present when the subject is idle. Although context awareness data is process in the feature extraction engine, no feature is extracted but only pre-processing and fusion is done.

6.2.5 Biometric Profile Template Generation

The fusion of in the framework is done in two stages before the classification of the biometric templets as stated in chapter 5. The feature is fused together within each of the three category data group. This is done after their features and normalisation is done for each extracted feature set. All feature set within the active, non-active and the combine normalised feature templates are fused together as a single feature template of active, non-active and combine feature templates for transmission to the biometric profile engine. The context awareness data is fused together separately in three categories of active, non-active and combined context awareness data template to be transmitted to the biometric profile engine too.

It applies many profile agents to process each of the biometric profile templates. As stated earlier, the feature templates should be reasonable enough to achieve the level of performance required. The feature template requirement for a reasonable level should meet the requirement detailed in the data extraction section. This suggests the biometric profile engine should only process templates that meet this requirement. On achieving the required amount of feature frames, the biometric profile engine begins to generate the profile for all the algorithms. The engine generates the biometric template using the 1,200 frames from the feature templates. The templates received from the feature extraction engine include the combined, active and non-active feature templates and the context awareness data templates. All the feature templates of every bioelectrical signal within each of the categories are fused together into biometric profile template while the contextual data is fused too in context awareness data template. The biometric profile templates and the context awareness data is stored temporary before forwarding it to the classification engine by the biometric profile controller. The algorithm template with successful classification is stored in the biometric profile storage. The biometric profile template is referred

to the classifier for re-classification. The biometric profile table as illustrated in Table 6.7 is designed to update the biometric profile templates with new intakes and discard old ones.

Table 6. 7: Biometric Profile Table

ID	Retrain date	Template	EER	Threshold value	Template
1	01/01/18	Active	0.27	0.21	\\biometricprofile\active
2	05/01/18	Non-active	2.04	1.6	\\biometricprofile\non-active
3	07/01/18	Combine	2.4	2.0	\\biometricprofile\combine

The verification is based upon how old the biometric profile is validated and stored. The older the biometric profile the higher the number associated with it i.e. if a biometric profile is newly validated and stored, a labelled 0 is attached to it and 1 when it is the second day. On the 7th day, with new templates generated the old templates with label 8 are discarded. This will depopulate the system and only retain recent templates. It will also help to alleviate the changes due to aging but for health, it is expected that the bioelectrical signal pattern will change rapidly which will lead to denial of access to the device. This can be resolve using a knowledge base method information store at the beginning to reset the system till the system is updated with new profile templates sufficient for subject's re-authentication. To successfully train a subject's template accurately, an impostor data is required. The biometric templates and the impostor's data are used to calculate the EER for each subject. The impostor data is preloaded at the installation of the framework implementation. The profile template as demonstrated in section the 5.2.4 is divided into one set for training and the other for testing. The subject's training data (from the biometric profile template) and an impostor data are trained with the classifier using neural network to obtain the EER. The optimal EER threshold is stored in the biometric profile table with the EER. Taking security and usability into consideration, the threshold setting to allow a subject to access the system is important. The subject is at liberty to choose the security level

setting depending if using the unified or static security setting. Security and usability consideration should be in the framework using the unified security setting, therefore, the threshold is set by the subject to create room for flexibility as describe in section 5.5.1. The result from chapter 5 is used to determine the bases for the threshold scale. The lower the threshold, the better the system while increasing the threshold allows room for impostor to access the system. Therefore, as the security increases there is the likelihood that more genuine subjects will be rejected while reducing the security level will also allow for impostor to be accepted by the system. The threshold as indicated in Table 6.8 shows the different levels of the security and correspondent EER (%) threshold.

Table 6. 8: showing different security level

Security Indicator	**5**	**4**	**3**	**2**	**1**
Security Level	Very High	High	medium	Low	Very Low
EER (%)	0.2	0.4	0.6	0.8	1.0

The threshold setting is in two folds, a unified and dynamic setting. The threshold indicates five level setting from very high (level 5) to very low (level 1) with the default level as medium (level 3). The unified threshold setting is set manually while the dynamic setting is executed by the framework if chosen as the preferred option. The threshold on the biometric profile table defines if the subject will be authenticated or not. If the classification output exceeds the threshold, the subject will be rejected from accessing the device. The output result if positive in authenticating the subject, the biometric profile template is logged on the biometric profile table and stored in the biometric profile storage for subsequent re-training of the subject. With a continuous verification of subjects, it is expected that the biometric profile table will be updated to provide for more recent samples while the samples rejected will be deleted.

6.2.6 Classification Engine

The Classification Engine as demonstrated in Figure 6.5 main function is the classification of the subjects. The classification of the input templates is on a continuous interval therefore running in the background continuously. The classification uses the biometric profile templates from any of the three algorithms depending on the algorithm that the biometric profile belongs to that is to be classified. This is done by using the biometric profile template from the biometric profile engine and impostor data stored in the biometric profile storage to classify a subject. The classification engine is updated on continuous bases as long as biometric profile engine generates the biometric profile templates, thereby using the most recent biometric profiles generated for the classification.

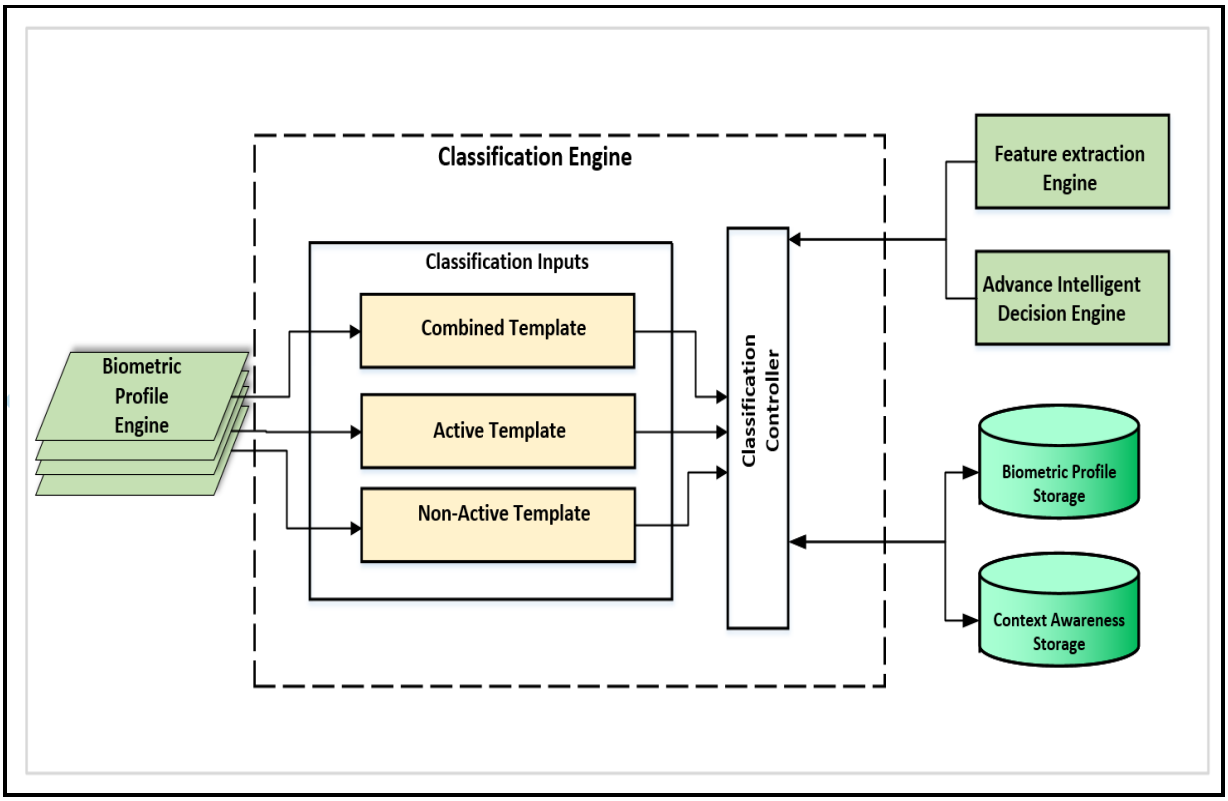


Figure 6. 5: Classification Engine

The authentication of subjects can be an onerous task because if an impostor accesses the phone, the impostor might cause much devastation to the content on the phone. When the classifier receives the biometric profile template to classify the subject appropriately, the activity manager is employed to know the activity the subject was engaged in at the time of extraction. Therefore, request is made for a template from the biometric profile storage that is suitable to classify the subject.

The classification algorithms are use as single algorithm. The most suitable algorithm is presented for classification by identifying the activity the subject is engaged with during extraction. To identify the activity, the classifier looks up for the template in the biometric profile storage for the template with similar input template for classification. The subject during extraction will be either in motion or not motion that means either the active or non-active

algorithm should be suitable at any time but when neither of the two could be suitable the combine algorithm is used. The combine algorithm contains both the active and non-active algorithm characteristic therefore can be use when needed for authentication. The activity is indicated with three motion types while the non-activity is indicated by one non-motion type. Therefore, if any of the templates is requested, the classification engine sends a request to the activity manager. The activity manger using the information provided by the classification engine sends the needed information for the classification engine to request the appropriate profile template from the profile template storage. The decision to reject or accept a user after classification is depended on the decision scheme rules. The Majority voting decision schemes has been decided in chapter 5 to apply for this research work. The majority voting will be applied before the outcome will be sent to the AIDE for further verification as proposed. The condition for the AIDE to do further verification of the outcome from the voting scheme will be discuss in the next section.

6.2.7 Advance Intelligent Decision Engine (AIDE)

The ubiquity of most of the smartphone in the market today provides the bases for context awareness extraction (Wright, 2009). Context awareness is becoming dynamic with personalization of application by extension the smartphone. The implicit interaction between the smartphone and the user has provided a platform for various context applications to achieve a define purpose. It can be used for accessing the user's environment because of the smartphone's ability to recognize and interpret their environment (Schmidt et al., 1999). This is the basis of introducing the Advance Intelligent Decision Engine (AIDE) as illustrated in Figure 6.6 to increase the decision accuracy of the proposed framework.

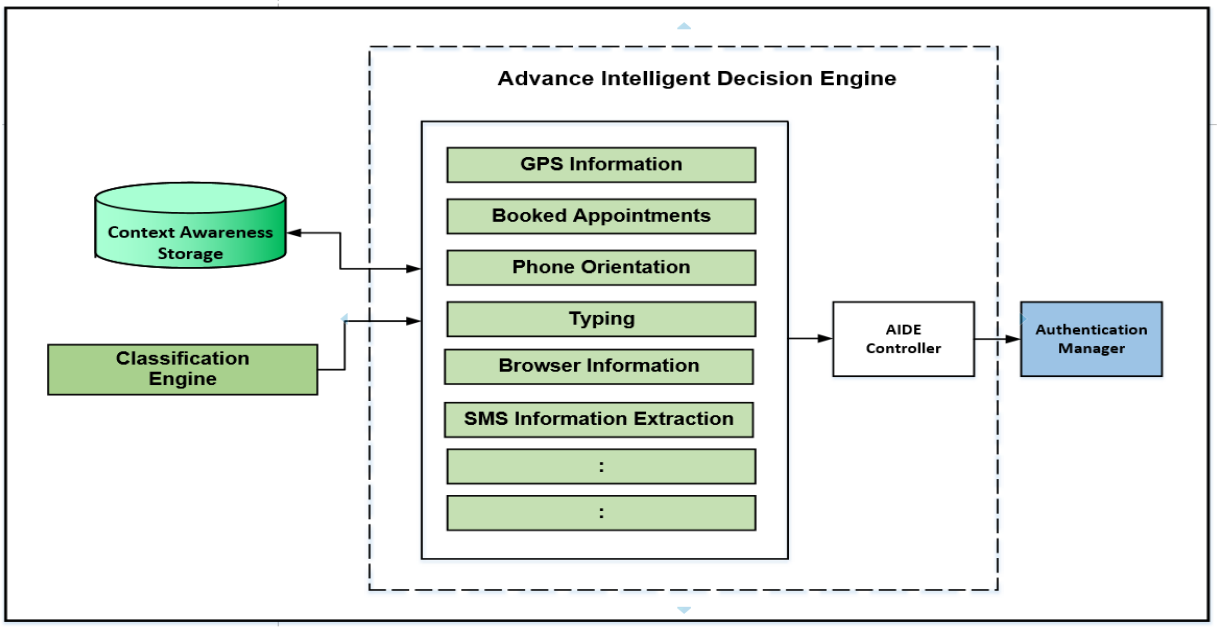


Figure 6. 6: Advance Intelligent Decision Engine (AIDE)

The Advance Intelligent Decision Engine (AIDE) is implemented with the aid of context awareness information mainly extracted from the subject's phone. It employs a number of context awareness information which includes the GPS information, the subject's detailed appointment stored on the phone's calendar, extracts information from the subject's Short Massaging Service (SMS) like appointment dates, venue and time, recognise subject's phone orientation when in use, know the typing style of the subject and the subject's logged steps, altitude etc. recorded by the smart watch. The availability of applications for social networking provides an avenue to study the subject's social online interaction pattern, therefore, it can be utilised as contextual information too.

To increase the guarantee that only the genuine subject should be allowed to access the device, the AIDE engine is used to enhance the classification output. The output scores from the classification result are collated and decision made using majority voting. The classification output is either accepted or rejected and is indicated as '1' or '0' respectively. The result from

the majority vote is used for authenticating the subject but as stated it is further verified by the AIDE depending on the output scores. The voting could be done using odd number from for 3 upward with the highest number of votes used to decide to accept or reject the subject (i.e. if the majority use 5 outputs and four out of the five classifications exceeded the threshold, the majority vote will be '1' that means the subject is authenticated with a score of '4'). The total result score of either '1' or '0' is sent to the advance intelligent decision engine through the classification controller. For quicker authentication process, if the classification scores 5 '1's, the AIDE will not verify the subject but send the output to the authentication manager. If the scores are 3 or 4, then there is further verification by the AIDE. Further action by the advance intelligent decision engine depends on the scores. The system sees the scores from the classification output as either pass with need for further verification or pass with no verification needed. This reduces the authentication processing time by forwarding the result to the authentication manager by the advance intelligent decision engine. This will increase the security level without much impact on the usability. The result from the classification is sent to the advance intelligent decision engine (AIDE) by the classification controller for further verification. The contextual information is employed by the AIDE to further decide if to the subject is genuine or an impostor. The addition of the AIDE increases the possibility of reducing the amount of impostor allowed accessing the device compared to what is obtainable presently.

The AIDE can seamlessly extract information from the phone, store relevant ones, evaluates and analysis the information and make intelligent decision to support the authentication process. The process should be flexible not relying solely on a defined way of extracting the information but using as many as possible parameter to make decision. For example, when a subject is skipping, the activity splitter might log the subject as running instead of jogging. This might be possible

because the stride taken by the subject is fast therefore, the extracted information at that time will be logged wrongly on the table. The AIDE should be able to alleviate the situation by applying context awareness to enhance the result for accurate authentication. The GPS information could help the system to analysis the output by sensing the subject is considerably in a location because there is no change of geographical location form the first location when the event started. With this verified by AIDE, the subject is accurately profiled. The AIDE while verifying a subject's will discover the location (most probably the subject's home or gym location GPS location when known by the AIDE) is accurate, the last browsing pattern suggest the subject is genuine and other parameters also accurately suggest the subject is in a known location. Therefore, if these locations are known by the AIDE, the framework will grant access to the subject. To understand the aim of the AIDE, different scenario will be used to illustrate the application of the AIDE in the proposed framework.

- **The application of GPS by the AIDE**: GPS sensors are fitted in most of the recent smart phones, this can be utilised to enhance user authentication. GPS could be used to track subject's daily route or movement pattern and location at a time in the day. This could also be done without internet using a pre-loaded GPS map used for navigation. It is anticipated that at certain time of the day during the week, a subject is expected to be regular in a location depending on the nature of the subject's daily routine. For example, if a working subject report for work at 9am and it takes about one hour from the house to work with a public bus, the bus leaving the bus stop by 8: 10am and the subject leave home at most 8am to meet up the bus. If the AIDE detects the subject leaving home (using the GPS tracker) by 8:05am, the AIDE expects the subject to be in a hurry, thereby running to catch up with the

bus. Any verification at that time will explore the active template characteristic to verify the subject by looking up for the template with the same characteristic. Also, the route can be used to verify the subject at a time of the day. The GPS could also improve the verification of the subject when in a moving vehicle if such subject's route is relatively the same at a time of the day. Also, the home or work place can be used to for verification; GPS information is fairly stable within a radius of that location.

- **Extraction of useful information from SMS and subject's appointment recorded on the phone:** The use of Short Messaging Service (SMS) is a popular medium of communication between mobile phones users. SMS messages as the name suggest are short messages therefore, the main reason a message is sent is highlighted without many pleasantries. It should be noted that researchers through forensic examination extracts useful information from the phone (Murphy, 2011). Some of the messages could contain information for appointment, invitation to a program etc. with the date, time and place of the event. Also, some subjects use their phone calendar to record appointments with a reminder to prepare ahead for the event. Important feature from these messages like time, date and place can be extracted by the AIDE to predict the subject location on the day and time of the event. This will help to verify the subject on that day and time if the subject is present at the venue. When verifying the subject on that day, though the GPS location not associated with the subject in the AIDE as a regular location. The GPS verification will indicate the subject is most likely to be in the location so will authenticate the subject on the GPS verification as pass. If the subject's location is not or never being associated with the subject and no information about the location, the GPS verification will fail to authenticate the subject. The

AIDE could also know if the subject is late to the event when the subject leaves his present location few minutes to the time of the event if the subject is attending the event. It could be used to predict the motion type or route of the subjects if the subject is heading toward the direction of the event by the tracker.

- **Identifying subject through phone touchscreen and orientation pattern:** with the advent of smart phone, the opportunity it provides is enormous which has made it popular. The availability of acceleration sensors on mobile phones has enhanced phone orientation detection(Carlson et al., 2015). The accelerometer uses the x, y and z position to record the position and rotation of each axis of the phone. The phone orientation is a source for context awareness extraction for identification purpose (Incel, 2015). The way the subject uses the phone while receiving or making a call, typing a message or browsing is unique to the subject. The phone touchscreen is the action of tapping the phone with the finger to navigate through the phone. The pattern of tapping and interaction with the phone crease adequate distinctive values associated to the subject (Antal and Szabó, 2016). The AIDE can store the value attributed to the orientation or the touchscreen pattern of the phone. This can be used to assist the final verification of the subject if the stored attribute is the same with the input value.

- **The subject's typing style:** the typing pattern of a subject has been used for authentication purpose by researchers (Araújo et al., 2005, Campisi et al., 2009b). To write a message or browse on the phone, the subject involves typing. The AIDE also captures the keystroke of the subject to use for enhancing the classification result.

- **Online Social Network (OSN) activities and subject browsing pattern:** Online social networking is popular with 10% of time spent online by smartphone users are engaged in online social network activities either for professional contact (LinkedIn, Facebook, MySpace) or socialising (whatsapp, snapchat) (Benevenuto et al., 2009). The browsing pattern of the subject is important in understanding how different subjects interact online. The online social network and the non-online social network activities log entry can be used to further strengthen the verification of the classified result by the AIDE.

- **Steps:** the steps of the subject are extracted from the smart watch. This has earlier been proven to enhance user authentication. It could also be used as gait recognition of the subject as discussed in chapter 5.

The context awareness information discussed will be used to enhance and verify the classification result. The AIDE employs intelligent information gathering from each of the contextual information, score them and apply the outcome to decide on the validity of the classification result.

The AIDE gets the output result from the classification engine, looks up for the context awareness table to verify if each contextual information (AIDE activities of the subject) on the table matches with the classification out template. It does this by scoring each of the five (depending on the number of context awareness information available) output template used after verifying the subject contextual characteristic using the context awareness table. The AIDE analysed and evaluates the contextual information then assigns a numeric value to the context awareness data associated with the algorithm template. For example, if the AIDE verified that

the subject is at a particular location at a certain time which is a usual location the subject is at that time of the day, the AIDE appends '1' (which show the verification is successful) to the GPS information for that template. If the subject is in a location that cannot be verified by the AIDE, it appends a '-1' (which show the verification is not successful) to the GPS while if no information is found for the GPS at that time it appends '0' (which show there is no information) as illustrates Table 6.9. The total score output form the contextual evaluation must be above 50% of the cumulative value of output. The outcome of the AIDE is forwarded to the authentication manager. The AIDE could send the classification output if the five classification results are '1's to the authentication manager because the subject is perfectly classified as a genuine subject because the five outputs are all positive results. The classification and AIDE result are presented in a table as illustrate by Table 6.9 and 6.10. The table is for illustration but in real implementation, it is expected that within the 15 seconds (each output 3 seconds) the subject will be activity will be stable therefore, the valve across the 5 outputs might be the same or with little differences.

Table 6. 9: Context Awareness Score Table

Context awareness	Output 1	Output 2	Output 3	Output 4	Output 5
GPS	1	1	1	1	0
SMS/Calendar	1	1	1	1	1
Touchscreen/orientation	1	1	1	0	-1
Typing style	1	-1	1	1	0
OSN/browsing pattern	0	1	1	-1	1
Steps	1	1	1	1	1
:	:	:	:	:	:
Score	**5**	**4**	**6**	**3**	**2**

Table 6. 10: Biometric Authentication Table

ID	Date	Time	Template	Classification Performance	AIDE Performance
1	4/04//2018	10:02	Active	5	5
2	4/04//2018	10:03	Non-active	4	5
4	4/04//2018	10:08	Combine	3	5
:	:		:	:	:

As stated earlier, the context awareness table stores the contextual information in the context awareness storage. When a classification is made, the output data is received by the AIDE. The AIDE also employs a majority voting base on the result from the Context Awareness Score Table.

6.2.7 Activity Manager

The activity manager's duty is to provide information on the activity the subject is engaged in at any time of data extraction. The activity manager gets its information from the data extraction engine via the activity splitter. The activity splitter after slitting the data in the data categories, it sends the activity information with activity type and time to the activity manager. The activity manager communicates with the classification engine and the AIDE to provide information on which activity type is most suited for any presented template. This will help the classifier to identity the template to request for from the biometric profile engine for authentication. There are four activity types; three are for the motion while one is for the non-motion activity see Table 6. 1: Activity Identification Table. The active templates might contain different motion types therefore the activity manager assist any request from either the classification engine or the AIDE.

6.2.8 Authentication Manager

The Authentication Manager makes the final decision of authentication of the BEBR framework to accept or reject a subject. The main role of the authentication manager is to makes decision of subject's authentication after receiving the result information from the classification result and the advance intelligent decision engine. The authentication manager utilises the advance intelligent decision engine by relying on the information provided by the biometric

authentication table and context awareness score table to make the decision of either grant access or reject the subject to access information on the phone. The process of the usage of the framework mechanism starts by requesting the subjects to register knowledge based details as explained in the last section. The built-in authentication mechanism of the phone is used till data collection to meet the BEBR framework requirement to activate its implementation. The knowledge base information is also used to restart the authentication when a genuine subject is log out of the system resulting from failed authentication. It could also be used to re-set the BEBR user authentication system if the subject stops using the mechanism for a specified period. After reset, the BEBR authentication process starts all over again. The inbuilt authentication mechanism is used till the BEBR meet the requirement to be activated.

The authentication manager also evaluates the security of the framework by regulating the authentication threshold (security level) to use for each algorithm. Another function includes the general feedback information to the subject about the security performance of the threshold used. It shows the different performance of both the classification output and the AIDE result for the subject. This will help the subject with information on the activity or context awareness information contribution to accurately authentication the subject. This information provides more useful assistance to enhance the authentication process by further verifying the identity of subject if subsequent activity or context awareness output result is low compare the its usual trend. It also monitors how secure the system is and able to provide the necessary check to accept the subject or deny the unauthorised subject. To determine the level of security of the system security evaluation component depends on how often a genuine subject is authenticated and the threshold used. The value ranges from 0 to 5. While 0 indicate that the classification output

above 10% EER, 5 indicate the strongest security level as illustrated in Table 6.11. The security level is set a 0 at the beginning of the BEBR system.

Table 6. 11: Authentication factor

Performance of Authentication	Authentication factor
0 – 0.2%	5
0.2 – 0.4%	4
0.4 –0. 6%	3
0.6 –0. 8%	2
0.8 – 1.0%	1
1.0% >	0

6.2.9 Storage Database

The BEBR framework us many different tables, most of this tables are generated as the subject's bioelectrical signals are extracted. The tables are mostly use to store information in their various engines for a short duration and discarded them after a limited period of time. The storage database contains two data bases that include the context awareness and biometric profile storage. The context awareness storage is used by the classification and Advance Intelligent Decision Engine (AIDE) engines while the biometric profile storage is used by the classification and authentication manager. The input source for the context awareness storage is from the data collection engine that extracts the activities with time stamp, data and the motion type of the activity. This information is stored on the activity identification table and is used by the authentication manager. Context awareness table stored in the biometric awareness storage is used by the classification engine to identify the activity the subject is engaged in at the time of the signal extraction. This information will help the classifier to know the most appropriate algorithm to use by looking at the activity ID from the activity identification table compare with the extracted activity ID. (i.e. if any activity ID is only present in the template, that corresponding extracted template is used for classification). The knowledge base information

table is used initially for user authentication up till when the BEBR framework mechanism is adopted. A subject may not use the framework for a long period of time and the system updating for subject profile has exceeded the required length of time for the BEBR framework to generate a new biometric profile template. Therefore, the knowledge base authentication as illustrate in Table 6.12 is activated to make sure the subject that about to reuse the mechanism is the former user of the phone and wants to re-use the mechanism. Table 6.12 illustrate the authentication information need to re-authenticate a subject to re-use the mechanism.

Table 6. 12: Knowledge base Information Table

Subject Information Stored	Subject's answers
Email	flourish@favour.com
1. What is your first pet	Jack
2. What is your favourite colour	Skye blue
3. Which town is your favourite park located	Yenagoa
4. What is your favourite food	Jollof rice
5. PIN	1234
:	:

Table 6. 13: Authentication Table

ID	Date	AIDE Result	EER (%)	Algorithm	Location
1	01/01/18	3	2.4	Combine	\\authentucation\combined
2	05/01/18	4	2.04	Non-active	\\authentucation\non-active
3	07/01/18	6	0.27	Active	\\authentucation\active
:	:	:	:	:	:

6.3 Conclusion

Most of the frameworks develop to improve the use of transparent method to verify a subject fall short of increasing the user's convenience. In this framework, the user convenience is considered along security. The user's convenience not withstanding did not hinder the improvement of the security desired. This research further increased the security level by incorporating an intelligence agent into the framework (the AIDE). This is expected to reduce the failure rate of authentication a genuine subject base on addition contextual information. The framework also

considered the intrusive nature of user authentication by making the framework non-intrusive. This approach will improve the overall user experience of smart mobile device because the mobile user will pay less attention on the intrusive nature of login presently in practice and still achieve a good level of security.

7. Evaluation of Bioelectrical Body Recognition Framework

7.1 Introduction

This chapter evaluates the performance of the Bioelectrical Body Recognition (BEBR) framework as proposed in the preceding chapter. The BEBR framework is evaluated through simulation based upon the previously captured user data (the testing dataset) used for classification in Chapter 5. The simulation employed a multi-algorithmic approach and different security levels also drawn from the methodology in Chapter 5 for the evaluation. The architecture of the proposed framework in Chapter 6 effectively allows part of the architecture to manage and process the output of the classifier to make a decision for the Bioelectrical Body Recognition (BEBR) framework. Therefore, to evaluate the performance of the BEBR framework, the following objectives where created:

- To investigate the performance of the classifier using different security level settings of the proposed architecture
- To investigate the impact of majority voting on the classification output using different security levels across different authentication windows

To achieve the objectives, six scenarios are created as illustrated in Table 7.1 and divided into pre-majority voting and post-majority voting scheme evaluation. The three simulations in each of

the sections used the three algorithms of combined, active and the non-active with the EER obtained in chapter 5.

Table 7. 1: The scenarios for the simulation process

Scenarios	Simulations	EER
A	Simulation of the Combined Algorithm performance for all security levels	3.4%
B	Simulation of the Active Algorithm performance for all security levels	2.04%
C	Simulation of the Non-Active Algorithm performance for all security levels	0.27%
D	Simulation of the Combined Algorithm applying voting scheme for all security levels	-
E	Simulation of the Active Algorithm applying voting scheme for all security levels	-
F	Simulation of the Non-Active Algorithm applying voting scheme for all security levels	-

7.2 Methodology

To stimulate the different scenarios, the subjects are divided into genuine subjects and impostors. The simulation used 30 subjects, the same as the subjects used in section 5.2 for the experiment. From the experiment carried out in Chapter 5, MATLAB scripts is used to classify the dataset with the dataset divided into training and testing dataset. The test data from that experiment is used for the evaluation in this section. From the 30 users, one subject is used as a genuine subject while the other 29 subjects are seen as impostors. This is done across all the 30 subjects acting a genuine subject. To authenticate a subject after classification, the subject's classification output score must exceed a set security level. In creating the scenarios, all the algorithms are evaluated with all the 5 security levels as illustrated in Table 7.2 to determine the FRR, FAR and percentage of acceptance or rejection in each level of security setting.

Table 7. 2: Security levels and their corresponding EER (%) setting for static setting

Security Indicator	**5**	**4**	**3**	**2**	**1**
Security Level	Very High	High	medium	Low	Very Low
Threshold	1.0	0.8	0.6	0.4	0.2

To improve the performance of the framework, a majority voting is introduced. Every input sample is made up of 3 seconds; therefore for the various input samples used for majority voting will be the number of input samples multiplied by 3 seconds to create an authentication window as illustrated in the Table 7.3.

Table 7. 3: Majority voting scheme input and authentication window

Number	Input Samples	Authentication window
1	3	9 seconds
2	5	15 seconds
3	7	21 seconds
4	9	27 seconds

To authenticate a subject, the majority voting output to accept or reject the subject to access the phone is determined by the authentication manager. The authentication manager depends on the information provided by the classifier or the AIDE. The voting scheme authenticates a subject in any authentication window with a majority of the output samples that exceeds the threshold while rejecting a subject with output samples that did not pass the threshold.

7.3 Simulation Implementation

The simulation of the multi-algorithm across the security levels is to determine the effectiveness of the proposed BEBR framework. To achieve this, the False Acceptance Rate (FAR), the False Rejection Rate (FRR), the rejection and acceptance rate of genuine subjects and impostors are tabulated and analysed. The total simulation used 30 subjects as mention earlier with a subject used as a genuine subject within the thirty subjects while the other twenty-nine subjects as impostors.

To show a fair reflection of the framework performance, the simulation for each user is repeated for ten times across all the security levels. Therefore, a genuine subject attempts to access the device ten times while each of the 29 impostors attempts to access the device ten times. The total attempt for the genuine subjects and impostors are 10 and 290 times respectively. Therefore, using 30 subjects, the total possible number of attempts for an authentication window by the genuine subjects is 300 times and for the 29 impostors, it will be 8700 times. The application of majority voting in the simulation across the four authentication window using 30 subjects will see the number of possible attempt for genuine subjects and impostors increase to 1,200 times and 34,800 times respectively. The following formula is used for to calculate the FRR and FAR:

$$FRR\ (\%) = \frac{Number\ of\ genuine\ users\ rejected}{All\ possible\ Attempt\ to\ access\ the\ device\ by\ genuine\ subject}\ X\ 100$$

Equation 7.1: Calculation of the FRR

$$FAR\ (\%) = \frac{Number\ of\ Impostors\ that\ gain\ access}{All\ possible\ Attempt\ to\ access\ the\ device\ by\ impostor}\ X\ 100$$

Equation 7.2: Calculation of the FAR

7.3.1 Simulation of the classification output

The pre-majority voting scheme simulation is done with the direct output from the classification. This is to access the performance of the output without the application of a voting scheme. The False Acceptance Rate (FAR) and the False Rejection Rate (FRR) is analysed using the different security levels for both the genuine users and the impostors.

- **Scenario A – Simulation of the Combined algorithm performance for all security levels**

Table 7.4 show the combined algorithm simulation for the classification output. From the table, the FFR at level 1 has a showing of false rejection of genuine subjects but from the security level 2 down to the reject rate is high with 18% rejections while the rate of falsely accepting an impostor is less than 0.2% from the security levels of 3, 4 and 5. This shows good level in securing the framework from been access by an impostor but using any of these levels will mean high genuine subjects will be rejected.

Table 7. 4: Combined Algorithm FRR and FAR performance

Simulation of the Combined Algorithm for all security levels		
Security Level	FRR	FAR
1	9%	5.6%
2	18.3%	1.6%
3	22.6%	0.2%
4	29%	0%
5	77.7%	0%

Table 7.5 shows the number of subjects either accepted or rejected as genuine or impostors. The rejection of genuine subject and its corresponding acceptance of impostor are not desirable. For example using the security level 3 with 2 impostors (0.2%) accepted to access the device is good in term of security but with the rejection of 68 genuine subjects, that is 22.6% is not good enough because it becomes a usability issue. The security level and the usability should be considered in choosing the appropriate security level to use.

Table 7. 5: Combined Algorithm performance

Combined Algorithm performance								
Security Level	**Genuine users**				**Impostors**			
	Acceptance		**Rejected**		**Acceptance**		**Rejected**	
1	273	91%	27	9%	49	5.6%	821	94.4%
2	245	81%	55	18.3%	14	1.6%	856	98.4%
3	232	77.7%	68	22.6%	2	0.2%	868	99.8%

4	213	71%	87	29%	0	0%	870	100%
5	67	22.3%	233	77.7%	0	0%	870	100%

- **Scenario B – Simulation of the Active algorithm performance for all security levels**

The active algorithm has a worst score than the combine algorithm in security level 1 with 13% FRR but performed better with the FAR for the same security level. This might be attributed to the fact that the active algorithm has more activities like walking, running, jogging etc. grouped together as active. The non-creation of algorithms for the different activities might reduce the identification rate for active algorithm. The other security level achieved better result than the combine algorithm.

Table 7. 6: Active Algorithm FRR and FAR performance

Simulation of the Active Algorithm for all security levels		
Security Level	FRR	FAR
1	13%	4.1%
2	14.3%	0.1%
3	16.7%	0%
4	19.3%	0%
5	68.7%	0%

The analysis of the number of genuine subjects rejected using the active algorithm is better from the security level 2 to security level 5. Though the number of rejection reduced compared to the combine algorithm, the amount 16.7% seems to be high for the security level 3 considering usability verses security.

Table 7. 7: Active Algorithm performance

Active Algorithm performance								
Security Level	**Genuine users**				**Impostors**			
	Acceptance		**Rejected**		**Acceptance**		**Rejected**	
1	261	87.0%	39	13%	36	4.1%	834	95.9%
2	257	85.7%	43	14.3%	1	0.1%	869	99.9%
3	250	83.3%	50	16.7%	0	0%	870	100%

4	242	80.7%	58	19.3%	0	0%	870	100%
5	94	31.3%	206	68.7%	0	0%	870	100%

- **Scenario C – Simulation of the Non-Active algorithm performance for all security levels**

The non-active active algorithm as illustrated in Table 7.7 and 7.8 has the best performance compared to the other two algorithms. With FRR of 1.3% using the lowest security level and 18.7% using the security highest security level shows the system achieved a better result considering usability and securing the system from impostors.

Table 7. 8: Non-active Algorithm FRR and FAR performance

Simulation of the Non-Active Algorithm for all security levels		
Security Level	FRR	FAR
1	1.3%	3.7%
2	8.7%	0.8%
3	11.7%	0.2%
4	11.7%	0.2%
5	18.7%	0%

The number of genuine subjects rejected by the phone dropped drastically to 4 subjects only for security level 1 while it reduce to significant level for the rest of the security levels. In term of usability verse security, level 2, 3 and 4 could be suitable for use because the percentage of rejection of genuine subject is seen to be good considering the percentage of accepting impostors.

Table 7. 9: Non-active Algorithm performance

Non-Active Algorithm performance								
Security Level	**Genuine users**				**Impostors**			
	Acceptance		**Rejected**		**Acceptance**		**Rejected**	
1	296	98.7%	4	1.3%	32	3.7%	838	96.3%
2	274	91.3%	26	8.7%	7	0.8%	863	99.2%
3	265	88.3%	35	11.7%	2	0.2%	868	99.8%
4	265	88.3%	35	11.7%	2	0.2%	868	99.8%
5	56	81.3%	244	18.7%	0	0%	870	100%

7.3.2 Simulation of the majority voting scheme application

The post- majority voting result is for comparison to access the impact of the majority voting scheme will have on the decision output. The different scenario presents a simulation using different authentication windows. The 9 seconds authentication window used 3 biometric profile samples for voting. The 15 seconds authentication window used 5 biometric profile samples, the 21 seconds authentication window used 7 biometric profile samples profile while the 27 seconds authentication window used 9 biometric profile samples for voting. The simulation is accessed across the 5 security level settings.

- **Scenario D – Simulation of the Combined algorithm applying voting scheme for all security levels**

Scenario D presents the result of the combine algorithm output from the application of majority voting. Table 7.9 and 7.10 shows the simulation output for the combined algorithm presented in term of FRR and FAR.

Table 7. 10: Majority voting simulation result for Combine Algorithm

Simulation of the Combined Algorithm for all security levels								
Security Level	**9 Seconds**		**15 Seconds**		**21 Seconds**		**27 Seconds**	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
1	9.7%	0.95%	9%	0.60%	8.3%	0.52%	8.3%	0.43%
2	18.3%	0.16%	16%	0.09%	14.7%	0.06%	15%	0.03%
3	22.7%	0.02%	22%	0%	22%	0%	23%	0%
4	29%	0%	29.7%	0%	28.3%	0%	28%	0%
5	77.7%	0%	81.3%	0%	83%	0%	84%	0%

The false rejection rate simulation for the combine algorithm shows the 21 and 27 seconds authentication window with security level 1 as the best. The worst is the 27 seconds authentication window with 84% of the genuine subjects falsely rejected when using security level 2. The FAR for the combine algorithm shows security level 4 and 5 for all authentication windows has no subject falsely accepted. This indicates that the two security levels can secure the phone from an impostor accessing the phone. However, using any of the security levels will have an effect on the genuine subject in term of convenience. This is because the best FRR within these levels is 28%, which is on the high side. To reduce the effect on a genuine subject's accessing the phone easily, the security level 3 will be considered to improve the user's convenience. The entire authentication window using the security level 3 scored 100% except the 9 seconds authentication window having 0.02% FAR with 22% FAR. The application of this security level mean there is the likelihood of no impostor gaining access to the phone if the authentication window of 15, 21 and 27 seconds is used. For the genuine subject been rejected is least with the 15 and 21 authentication window. This could be further seen in Table 7.7 with only 2 impostors accessed the phone on an average of the authentication window across the security level. This show the system is effective in rejecting impostor but genuine subject on the other hand has 269 out of 1200 attempts falsely rejected is high.

Table 7. 11: The Majority voting average perfomance for Combine Algorithm

Combined Algorithm average performance across all the authentication window								
Security Level	**Genuine users**				**Impostors**			
	Acceptance		**Rejected**		**Acceptance**		**Rejected**	
1	1094	91.2%	106	8.8%	217	2.5%	8483	97.5%
2	1008	84%	192	16%	30	0.3%	8670	99.7%
3	931	77.6%	269	22.4%	2	0.02%	8698	99.98%
4	855	71.2%	345	28.8%	0	0%	8700	100%
5	221	18.4%	979	81.6%	0	0%	8700	100%

Though the combine algorithm is only used when the active or the non-active is not suitable for presentation for classification. Therefore, using the combine algorithm is less frequent in the actual implementation of the framework. Taking the security of the phone into consideration while still considering the convenience of the subject using the framework, level 2 security is considered a the most suitable because the FAR of security level 2 using the authentication window of 15, 21 and 27 seconds is less than 1% just like the authentication window of 9 seconds in security level 2 that is 0.03%. This will also reduce the FRR to between 15% -18.3% increasing the convenience for the user.

- **Scenario E – Simulation of the Active Algorithm applying voting scheme for all security levels**

The simulation result for the scenario E as illustrated in Table 7.11 and 7.12 shows the summary of the FRR and FAR. The most suitable security level when considering usability is the security level 3, 4 and 5 which has 100% rejection of impostor, but the rejection rate of genuine user at the same levels has the best as 16.5%. The 16.5% of rejection at the security level 3 is good and the security level 2 is also good as 99.99% of impostors are rejected which approximately 100%.

Table 7. 12 : Majority voting simulation result for Active Algorithm

Simulation of the Active Algorithm for all security levels								
Security Level	**9 Seconds**		**15 Seconds**		**21 Seconds**		**27 Seconds**	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
1	13.0%	0.4%	13.33%	0.3%	13.33%	0.34%	13.33%	0.32%
2	14.33%	0.01%	15%	0%	14.33%	0%	14.33%	0%
3	16.33%	0%	16.67%	0%	16.33%	0%	16.33%	0%
4	19.33%	0%	18%	0%	18%	0%	18%	0%
5	68.67%	0%	71.33%	07%	72.67%	0%	73.67%	0%

Table 7. 13: The Majority voting average perfomance for Active Algorithm

Active Algorithm performance								
Security Level	Genuine users				Impostors			
	Acceptance		Rejected		Acceptance		Rejected	
1	1041	86.7%	159	13.3%	124	1.4%	8576	98.6%
2	1036	85.5%	164	13.7%	1	0.01%	8699	99.99%
3	1002	83.5%	198	16.5%	0	0.00	8700	100%
4	980	81.7%	220	18.3%	0	0.00	8700	100%
5	341	28.4%	859	71.6%	0	0.00	8700	100%

The rejection of genuine subject at the security level 2 is 13.7% that is better to consider compare to 16.5% of the security level 3. Therefore, the security level 2 could be used for the active algorithm to authenticate a subject. The average performance across the entire authentication window for the active algorithm level 2 as illustrated in table 7.10 shows 13.7% rejection of genuine subject, which is a good performance than the combined algorithm. The false rejection of genuine subject's attempt to access the phone using the active algorithm has a better performance than the combined algorithm. The FRR shows the best is 13.0% while the worst is 73.67% but in comparison with the combine algorithm, using the security level 2 will improve the FRR while the FAR will still be below1%

- **Scenario F– Simulation of the Non-Active algorithm applying voting scheme for all security levels**

The scenario F result as illustrated in Table 7.13 and 7.14 is shows it has the best performance compared to the other algorithms. The FRR scored above 15% (the best for the combine and non-active) from security level 4 and 5 while FAR has less than 1% just like the security level 2

in the combine and active algorithms. The aim is to consider usability as well as the security of the framework therefore, using the security level 2 as the others will improve the rejection of a genuine subject access to the phone to a maximum of 8.67% and the FAR to less than 1% which is the same across all the algorithms.

Table 7. 14: Majority voting simulation result for Non-active Algorithm

Simulation of the Non-Active Algorithm for all security levels								
Security Level	9 Seconds		15 Seconds		21 Seconds		27 Seconds	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
1	1.33%	0.37%	1%	0.11%	1.33%	0.06%	1.67%	0.02%
2	8.67%	0.08%	7%	0%	7.67%	0%	7%	0%
3	11.67%	0.02%	10%	0%	10.33%	0%	10%	0%
4	18%	0.02%	16.67%	0%	16.33%	0%	17%	0%
5	80.33%	0%	80.67%	0%	80%	0%	82%	0%

The analysis looking at the general performance across the authentication window on average within the level 2 show that 7 impostor's attempts to access the phone succeeded. Therefore, increasing the security level to 3 will reduce the average scores to 2 impostor's attempt succeeding as illustrated in table 7.14. Though the number of genuine subjects denied access increased, preventing minimal access to the phone by impostor should be more important. The FRR of the security level 3 has the maximum of 11.6% while the FAR on the same level has 0.02% which is better than the combine and active algorithms security level 2. The use of security level 3 for the non-active algorithm did not only improve the security compare the combine and the active algorithm but the convenience to the user is not affected as the FAR is still below the 1% performance as the other two algorithms.

Table 7. 15: The Majority voting average perfomance for Non-active Algorithm

Non-Active Algorithm performance								
Security Level	Genuine users				Impostors			
	Acceptance		Rejected		Acceptance		Rejected	
1	1184	98.7%	16	1.3%	49	0.6%	8651	99.4%
2	1109	92.4%	91	7.6%	7	0.1%	8693	99.9%
3	1074	89.5%	126	10.5%	2	0.02%	8698	99.98%
4	996	83%	204	17%	2	0.02%	8698	99.98%
5	231	19.3%	969	80.7%	0	0%	8700	100%

Analysing the performances across all the authentication window verses all the security levels with give a better insight into the performance of the framework therefore, the best from each security level has been identified but the authentication window for used is not. The average performance of the authentication window for the FRR shows the best performance in each of the algorithm of combined, active and non-active as 31.3%, 26.33% and 23.06% respectively. While this performance in noticed at different authentication windows, the FRR average performance across the three algorithms is in the same authentication window of 27 seconds. The security level to use in any of the algorithms differs but the authentication window should be the same across all algorithms. Therefore, to select a suitable authentication window across all the algorithm consideration should be given to the FFR that have the best average across different authentication window. For the combine algorithm, the FRR best average is 31.3% using the 9 seconds authentication window but using the selected security level 2, the FRR is 14.7%. The scores for the 27 seconds for the security level 2 is 15% which is 0.3% less compared to the 14.7% of the 9 seconds authentication window. Therefore, 27 seconds authentication window could be considered for use.

The active algorithm best average score is when the 9 seconds authentication window is used with the security level 2, the total score for the same level is 14.33%. It is interesting to note that

the 27 seconds authentication window on the security level 2 scores is the same for the 9 seconds authentication window using the same security level therefore, considered as the authentication window for the active algorithm. The non-active algorithm just like the active algorithm has the same score between the best average score using the authentication window of 15 seconds and the 27 authentication window using the security level 3 (the level selected for use). With this analysis, it will be concluded that the FAR authentication window using the 27 seconds across the entire algorithm performance better compared to any other authentication window.

In conclusion, the security level for use differs with the combine and the active using the security level 2 while that non-active uses the security level 3 with all algorithms using the 21 seconds authentication window as the most suitable taking security and usability into consideration.

7.4 Discussion

A good authentication framework should accept a legitimate user while protecting the system from impostors. The convenience of using a mobile phone security mechanism should not limit the security expectations of the mechanism. The four-scenario simulation performance indicator is based on the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The FAR and FRR of the Combine Algorithm at the attained an EER of 3.4%, the Active Algorithm at the attain an EER of 2.04% and the Non-Active Algorithm attained an EER of 0.27% as shown in Figure 7.1, 7.2 and 7.3. From the simulation, it is observed that the FRR is higher than the FAR for all the different simulation. The FAR is high mostly using the low security level (level 2) and very low security level (level 1) but the other levels shows almost 100 rejections of impostors.

This is desirable for a good authentication system but on the other hand, the FFR should not be too high because it will affect the easy usage of the authentication system.

For the combine algorithm FAR across all authentication windows, there is slight increase in the performance as the sizes of voting simply increases. This is also the case for the entire algorithm in scenario B and C. This indicates improvement as the length of input samples for voting increases as it is seen in the average calculations. This is not the same for FRR; the active algorithm (scenario A) shows it decreases as the voting sample increases from 31.5% to 32% then to 31.7 for the 27 seconds authentication window. This is also the same for the active algorithm but the non-active increased for the 15 seconds authentication window. This is an indication that the majority voting improves with more of the samples present for voting. By utilising 9 biometric profile samples within the 27 seconds authentication window to achieve the presented result is good enough. This is because the 27 seconds authentication window means an authentication can be done twice within a minute taking advantage of the authentication window to provide effective continues authentication within a short interval. This will reduce the time an impostor in logged in to access the device. If access is granted and the user is an impostor, the next re-authentication will be in few seconds since it takes 27 seconds to extract the information need to re-verify the user (depending on the setting for authentication intervals).

The overall acceptance of impostors on the average is less than 1% however; the average rejection rate of genuine subjects is in the region of 31.52% to 23.42% brings about usability issues because many genuine subjects are rejected. To improve the security and usability of the authentication framework that is the aim of the research, the three selected security level for the three algorithms will improve the security. The performance of the legitimate user in term of

number of rejections across the various security levels shows the non-active algorithm as the best. With 126 genuine subjects rejected making it 10.5% using the selected security level 3 is still high but showed good scores compared to the other algorithms.

The application of majority voting has greatly enhanced the performance of the framework. The pre-voting simulation has relatively the same result with the post-voting simulation using 9 seconds authentication window across all the security level in all the algorithms. This might be because of the input sample for the pre-voting has a good number of samples used for the post-voting samples of 3 biometric profile samples used for the voting. However, the performance improves as the authentication windows increases but more on the FAR than the FRR, also on the simulation of majority voting application using the 21 seconds authentication window in comparison to the pre-voting simulation. The summery of the result using the 21 seconds authentication for the combine algorithm (security level 2) will be for FRR of 22% and FAR of 0%, the Active algorithm (security level 2) will be FRR of 14.33% and FAR of 0% while the Non-active algorithm (security level 3) will be FRR of 10.33% and FAR of 0%.

7.5 Conclusion

The evaluation of the novel Bioelectrical Body Recognition (BEBR) framework has shown that it could provide a secured and suitable user authentication system. The performance of the system achieved the aim of the research because it increases the usability with the selection of a suitable security level from the framework in respect to rejection of impostors and accepting genuine subjects. The acceptance of as many as possible genuine users may take away the usability issues but the design of the authentication architecture should prevent impostors from

been accepted by the system. To further improve the authentication framework, the majority voting scheme should be set by the framework. From the result from all the simulations it shows a good level of performance compare to the present authentication mechanism in place because the non-intrusiveness and transparency applied in the data extraction did not reduce the security performance. This will improve the framework in term of usability verses convenience, the higher the level the better the security of the device with a reasonable usability level while the low security setting is still considered good in terms of usability and security.

8. Conclusions and Future Work

This chapter discusses the achievements of the research work while highlighting the limitations too. The research aim is to authenticate subjects employing bioelectrical signals while considering the convenience of the use of the framework.

8.1 Contributions and Achievements of the Research

The research objective set out in chapter 1 has been achieved with several experimental studies and evaluation leading to the development of the Bioelectrical Body Recognition System (BEBR) framework. The contributions and achievements of the research are listed below:

- Undertook an elaborate literature review on transparent user authentication systems, identified the weakness and the need for a better user authentication mechanism that is transparent to the user while the issue of user convenience is considered.
- A technology evaluation is carried out using existing technology to extract bioelectrical signals and contextual data. The research achieved the collection of the largest volume of real life bioelectrical signals and contextual data.
- Investigated the viability of the bioelectrical signals and contextual data for transparent user authentication by applying multi-algorithm approach to the classification design. This is the first research work using smart watch for transparent user authentication employing a real live bioelectrical signals and context awareness in a large scale.
- Proposed a novel Bioelectrical Body Recognition framework to support the use of bioelectrical signals and contextual data within the framework. The framework employed an intelligent component to further strengthen the security while the non-intrusive method of data extraction enhances the user-friendliness and transparency of the framework.

- An evaluation is carried out through simulation under different scenarios of the multi-algorithm usage within different security levels. The simulation is carries out on a pre-application and post-application of a voting scheme to show the impact of the approach used to enhance the security to in the framework.

A number of papers relating to the research have been published and this is presented in Appendix A. This research has contributed positively to transparent user authentication for portable smart mobile devices.

8.2 Limitations of the Research

The research aim has been achieved but not without some issues. The issues had some impact on the work progress. The major limitations include:

- There was a limitation on a continuous collection of data on the smart watches without draining the battery. This was a limitation not been able to collect a full day's worth of data over the seven days period, which is what could have been preferred. The smart watches technology has limitation because it is not developed to be used in this fashion hence the technology evaluation to select the smart watch to achieve the aim of the research.
- Due to the nature of the data collection, there were not enough context base information and this lead to not been able to fully evaluate the framework applying the AIDE however most of the other component were used.
- There is limitation to fully break down the dataset base on subject's activities because most of the activities were sitting, walking with few subjects engaged in running. The lack of a

longer time for collection of the dataset prevented the research from taking variety of activities to further investigate the multi-algorithm approach.

The limitations notwithstanding, the research work is believed to have achieved its aims and made a reasonable novel contribution to knowledge in the field of transparent user authentication.

8.3 Suggestions & Future Work

This research has improved on the application of bioelectrical signals for a transparent user authentication however; there are areas for future work to be conducted employing bioelectrical signals. These include:

- The technology used for the extraction of the dataset is adequate for the research work however, a future work should look at the nature technology and implementation in order to minimise computer overhead and battery exhaustion both for the phone and the smart watch.
- A technique should be developed and investigation done to understand the optimal point on the best possible way to achieve maximal benefit of the technologies used.
- There is the need to further experiment on the ideal of context awareness information within the Advance Intelligent Decision process and understand the contribution it will have on the performance it has achieved.

8.4 Importance of Research Contribution

History has already demonstrated that the need for users to be authenticated is only increasing, with the burden now arguably at breaking point. More usable and convenient approaches are essential if security is to be maintained whilst not impacting the willingness to adopt these new

technologies. Recent advancements made by Apple in particular with the Touch ID and Face ID are exemplars into how to achieve secure but usable authentication. Also, there has been increase in the use of mobile smart devices for enhancing security in homes by devices syncing with home devices. However, issues still remain regarding the integration of these technologies across devices, technologies and services to enable a seamless and functionless experience independent of what and how the user is using a particular technology or service.

References

ABBOUD, A. J. & JASSIM, S. A. Biometric templates selection and update using quality measures. Mobile Multimedia/Image Processing, Security, and Applications 2012, 2012. International Society for Optics and Photonics, 840609.

ABE, N. & SHINZAKI, T. 2008. A Survey on Newer Prospective Biometric Authentication Modalities.

ABOWD, G. D., DEY, A. K., BROWN, P. J., DAVIES, N., SMITH, M. & STEGGLES, P. Towards a better understanding of context and context-awareness. International Symposium on Handheld and Ubiquitous Computing, 1999. Springer, 304-307.

ACUNETIX. 2014. *Weak Password Vulnerability: More Common than You Think* [Online]. London. Available: http://www.acunetix.com/blog/articles/weak-password-vulnerability-common-think/ [Accessed 2015].

ACUNETIX. 2015. *Acunetix clamps down on costly website security with online solution* [Online]. London. Available: http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/ [Accessed 25, march 2015].

ADDISON, P. S., WALKER, J. & GUIDO, R. C. 2009. Time--frequency analysis of biosignals. *IEEE engineering in medicine and biology magazine,* 28**,** 14-29.

AL-DARAISEH, A. A., AL OMARI, D., AL HAMID, H., HAMAD, N. & ALTHEMALI, R. 2015. Effectiveness of iPhones Touch ID: KSA case study. *Editorial Preface,* 6.

AL-WAISY, A. S., QAHWAJI, R., IPSON, S. & AL-FAHDAWI, S. A fast and accurate iris localization technique for healthcare security system. Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, 2015. IEEE, 1028-1034.

ALKHALDI, A. N. 2016. ADOPTION OF MOBILE BANKING IN SAUDI ARABIA: AN EMPIRICAL EVALUATION STUDY. *International Journal of Managing Information Technology (IJMIT),* Vol.8, .

AMAZE. 2014. *Digital commerce – How businesses achieve global success* [Online]. Available: http://www.amaze.com/Images/Digital_Commerce_Whitepaper_tcm22-5165.pdf [Accessed 10th November 2014].

AMBALAKAT, P. Security of biometric authentication systems. 21st Computer Science Seminar, 2005. Citeseer, 1.

ANDERSSON, D. & SAEDÉN, D. 2013. Authentication with Passwords and Passphrases - Implications on Usability and Security. Lund University School of Economics and Management.

ANTAL, M. & SZABÓ, L. Z. 2016. Biometric authentication based on touchscreen swipe patterns. *Procedia Technology,* 22**,** 862-869.

ARAFAT, S. & BELLEGDI, S. 2017. Automatic Detection of Epilepsy Using EEG Energy and Frequency Bands. *International Journal of Applied Mathematics, Electronics and Computers,* 5**,** 36-41.

ARAÚJO, L. C., SUCUPIRA, L. H., LIZARRAGA, M. G., LING, L. L. & YABU-UTI, J. B. T. 2005. User authentication through typing biometrics features. *IEEE transactions on signal processing,* 53**,** 851-855.

ATREY, P. K., HOSSAIN, M. A., EL SADDIK, A. & KANKANHALLI, M. S. 2010. Multimodal fusion for multimedia analysis: a survey. *Multimedia systems,* 16**,** 345-379.

AVILA, C. S. A., CASANOVA, J. G., BALLESTEROS, F., GARC´ıA, L. J. M. ı., G´OMEZ, M. F. A., SIERRA, D. D. S. & POZO, G. B. D. 2014. *State of the art of mobile biometrics, liveness and non-coercion detection* [Online]. Available: https://www.pcas-project.eu/images/Deliverables/PCAS-D3.1.pdf [Accessed 12/05/2015 2015].

BAHL, L., DE SOUZA, P., GOPALAKRISHNAN, P., NAHAMOO, D. & PICHENY, M. Robust methods for using context-dependent features and models in a continuous speech recognizer.

Acoustics, Speech, and Signal Processing, 1994. ICASSP-94., 1994 IEEE International Conference on, 1994. IEEE, I/533-I/536 vol. 1.
BARDRAM, J. E., BALDUS, H. & FAVELA, J. 2007. Pervasive Computering in Hospitals *In:* BARDRAM, J. E., MIHAILIDIS, A. & WAN, D. (eds.) *Prevasive Computer in healthcare.* USA: CRC Press.
BATTITI, R. & COLLA, A. M. 1994. Democracy in neural nets: Voting schemes for classification. *Neural Networks,* 7**,** 691-707.
BELLE, A., HARGRAVES, R. H. & NAJARIAN, K. 2012. An automated optimal engagement and attention detection system using electrocardiogram. *Computational and mathematical methods in medicine,* 2012.
BENABDELKADER, C., CUTLER, R. & DAVIS, L. Stride and cadence as a biometric in automatic person identification and verification. Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on, 21-21 May 2002 2002. 372-377.
BENEVENUTO, F., RODRIGUES, T., CHA, M. & ALMEIDA, V. Characterizing user behavior in online social networks. Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement, 2009. ACM, 49-62.
BHATTACHARYYA, D., RANJAN, R., ALISHEROV, F. & CHOI, M. 2009. Biometric authentication: A review. *International Journal of u- and e- Service, Science and Technology,* 2**,** 13-28.
BIEL, L., PETTERSSON, O., PHILIPSON, L. & WIDE, P. 2001. ECG analysis: a new approach in human identification. *Instrumentation and Measurement, IEEE Transactions on,* 50**,** 808-812.
BIOMTRICS, G. 2014. *Biometric System Model Modules* [Online]. Available: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/introduction/model/biometric-system-model [Accessed 30/01/2015].
BO-ZHI, F. & HONG-BIN, Z. Feature extraction using wavelet packet decomposition based on MPEG-I. Computer Science and Software Engineering, 2008 International Conference on, 2008. IEEE, 1048-1052.
BOARDOFGOVERNORS 2014. Consumers and Mobile Financial Services 2014. *In:* SYATEM, B. O. G. O. T. F. R. (ed.). Washington, DC 20551: Federal Reserve Board.
BONNEAU, J. & PREIBUSCH, S. The Password Thicket: Technical and Market Failures in Human Authentication on the Web. 2010.
BONO, V., BISWAS, D., DAS, S. & MAHARATNA, K. Classifying human emotional states using wireless EEG based ERP and functional connectivity measures. Biomedical and Health Informatics (BHI), 2016 IEEE-EMBS International Conference on, 2016. IEEE, 200-203.
BRAZ, C. & ROBERT, J.-M. Security and usability: the case of the user authentication methods. Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine, 2006. ACM, 199-203.
BRAZ, C., SEFFAH, A. & M'RAIHI, D. 2007. Designing a trade-off between usability and security: A metrics based-model. *Human-Computer Interaction–INTERACT 2007.* Springer.
BREIMAN, L. 1999. Random forests. *UC Berkeley TR567*.
BREIMAN, L. 2001. Random forests. *Machine learning,* 45**,** 5-32.
BUBECK, U. M. 2003. Multibiometric Authentication- An overview of recent development. *Term Project CS,* 574.
BULUSU, K. V. & PLESNIAK, M. W. 2015. Shannon entropy-based wavelet transform method for autonomous coherent structure identification in fluid flow field data. *Entropy,* 17**,** 6617-6642.
CACHIN, C. 1997. *Entropy measures and unconditional security in cryptography.*
CAMPISI, P., MAIORANA, E., BOSCO, M. L. & NERI, A. 2009a. User authentication using keystroke dynamics for cellular phones. *IET Signal Processing,* 3**,** 333-341.
CAMPISI, P., MAIORANA, E., BOSCO, M. L. & NERI, A. 2009b. User authentication using keystroke dynamics for cellular phones. *IET Signal Processing,* 3**,** 333–341.
CARLSON, C., CHEN, T., CRUZ, J., MAGHSOUDI, J., ZHAO, H. & MONACO, J. V. 2015. User Authentication with Android Accelerometer and Gyroscope Sensors.

CARROLL, A. & HEISER, G. An Analysis of Power Consumption in a Smartphone. USENIX annual technical conference, 2010. Boston, MA, 21-21.
CHAN, A. D., HAMDY, M. M., BADRE, A. & BADEE, V. 2008. Wavelet distance measure for person identification using electrocardiograms. *Instrumentation and Measurement, IEEE Transactions on,* 57**,** 248-253.
CHARMAN, R. A. 1990. Part 1: The Electric Cell. *Physiotherapy,* 76**,** 503-508.
CHATRA, A. S. Cognitive biometrics based on EEG signal. Contemporary Computing and Informatics (IC3I), 2014 International Conference on, 2014. IEEE, 374-376.
CHEN, G. & BUI, T. 2003. Multiwavelets denoising using neighboring coefficients. *IEEE signal processing letters,* 10**,** 211-214.
CHEN, Y. & LIGINLAL, D. 2008. A maximum entropy approach to feature selection in knowledge-based authentication. *Decision Support Systems,* 46**,** 388-398.
CHIOU, S.-Y. 2013. Secure method for biometric-based recognition with integrated cryptographic functions. *BioMed research international,* 2013.
CHUANG, J. 2014. One-Step Two-Factor Authentication with Wearable Bio-Sensors.
CIMATO, S., GAMASSI, M., PIURI, V., SASSI, R. & SCOTTI, F. Privacy-aware biometrics: Design and implementation of a multimodal verification system. Computer Security Applications Conference, 2008. ACSAC 2008. Annual, 2008. IEEE, 130-139.
CLAESSENS, J., DEM, V., DE COCK, D., PRENEEL, B. & VANDEWALLE, J. 2002. On the security of today's online electronic banking systems. *Computers & Security,* 21**,** 253-265.
CLARKE, N. 2011a. *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling,* London, Springer.
CLARKE, N. 2011b. *Transparent user authentication: biometrics, RFID and behavioural profiling*, Springer Science & Business Media.
CLARKE, N., S.M.FURNELL & REYNOLDS, P. L. 2002. Biometric authentication for mobile devices. *3rd Australian information warfare and security conference* Australia.
CLARKE, N. L. & FURNELL, S. M. 2005. Authentication of users on mobile telephones–A survey of attitudes and practices. *Computers & Security,* 24**,** 519-527.
CLARKE, N. L. & MEKALA, A. 2007. The application of signature recognition to transparent handwriting verification for mobile devices. *Information management & computer security,* 15**,** 214-225.
COLOMER GRANERO, A., FUENTES-HURTADO, F., NARANJO ORNEDO, V., GUIXERES PROVINCIALE, J., AUSÍN, J. M. & ALCAÑIZ RAYA, M. 2016. A comparison of physiological signal analysis techniques and classifiers for automatic emotional evaluation of audiovisual contents. *Frontiers in computational neuroscience,* 10**,** 74.
CONSUMER. 2015. *DON'T FEAR THE REAPER: TAX DAY IS COMING, BUT MOBILE BANKING IS HELPING CONSUMERS BALANCE THEIR BOOKS* [Online]. Available: http://www.nielsen.com/us/en/insights/news/2015/dont-fear-the-reaper-tax-day-is-coming-but-mobile-banking-is-helping-consumers.html [Accessed].
COONEY, M. 2012. *10 common mobile security problems to attack* [Online]. PCWord. Available: http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html [Accessed 15, Sept. 2014].
COUTINHO, D. P., FRED, A. L. & FIGUEIREDO, M. A. One-lead ECG-based personal identification using Ziv-Merhav cross parsing. Pattern Recognition (ICPR), 2010 20th International Conference on, 2010. IEEE, 3858-3861.
COVINGTON, M. J., FOGLA, P., ZHAN, Z. & AHAMAD, M. A context-aware security architecture for emerging applications. Computer Security Applications Conference, 2002. Proceedings. 18th Annual, 2002. IEEE, 249-258.
COVINGTON, M. J., LONG, W., SRINIVASAN, S., DEV, A. K., AHAMAD, M. & ABOWD, G. D. Securing context-aware applications using environment roles. Proceedings of the sixth ACM symposium on Access control models and technologies, 2001. ACM, 10-20.

CROSBY, M. E. & IKEHARA, C. S. Continuous identity authentication using multimodal physiological sensors. Defense and Security, 2004. International Society for Optics and Photonics, 393-400.
CRYPTOSMITH. 2002. *PASSWORD EXPIRATION CONSIDERED HARMFUL* [Online]. 2014. Available: http://cryptosmith.com/password-sanity/exp-harmful/ [Accessed 12/7].
CVETKOVIC, D., ÜBEYLI, E. D. & COSIC, I. 2008. Wavelet transform feature extraction from human PPG, ECG, and EEG signal responses to ELF PEMF exposures: A pilot study. *Digital Signal Processing,* 18**,** 861-874.
DAVIS, R. 1987. Robustness and transparency in intelligent systems. *Proceedings Human Factors in Automated and Robotic Space Systems, National Research Council, Washington, DC***,** 211-233.
DAYA, B. 2013. *Network security: History, importance, and future* [Online]. Available: http://web.mit.edu/~bdaya/www/Network%20Security.pdf [Accessed 10/12 2014].
DE LUIS-GARCíA, R., ALBEROLA-LÓPEZ, C., AGHZOUT, O. & RUIZ-ALZOLA, J. 2003. Biometric identification systems. *Signal Processing,* 83**,** 2539-2557.
DICKHAUS, H. & HEINRICH, H. 1996. Classifying biosignals with wavelet networks [a method for noninvasive diagnosis]. *IEEE Engineering in Medicine and Biology Magazine,* 15**,** 103-111.
DIETZ, M., CZESKIS, A., BALFANZ, D. & WALLACH, D. S. Origin-Bound Certificates: A Fresh Approach to Strong Client Authentication for the Web. USENIX Security Symposium, 2012. 317-331.
DMITRIENKO, A., LIEBCHEN, C., ROSSOW, C. & SADEGHI, A.-R. 2014. On the (in) security of mobile two-factor authentication. *Financial Cryptography and Data Security.* Springer.
DOURISH, P., GRINTER, R. E., DE LA FLOR, J. D. & JOSEPH, M. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing,* 8**,** 391-401.
DOURISH, P. & REDMILES, D. An approach to usable security based on event monitoring and visualization. Proceedings of the 2002 workshop on New security paradigms, 2002. ACM, 75-81.
DUGGAN, G. B., JOHNSON, H. & GRAWEMEYER, B. 2012. Rational security: Modelling everyday password use. *International journal of human-computer studies,* 70**,** 415-431.
EL-ABED, M. & CHARRIER, C. 2012. *Evaluation of Biometric Systems*, InTech.
ELISH, K. O., YAO, D. & RYDER, B. G. User-centric dependence analysis for identifying malicious mobile apps. 2012.
ESTES, A. C. 2014. *Beware of This Dangerously Convincing Google Docs Phishing Scam* [Online]. gizmodo. Available: http://gizmodo.com/beware-of-this-dangerously-convincing-google-docs-phish-1546278702 [Accessed 17/02 2015].
FABBRI, G., BOCCALETTI, C., CARDOSO, A. M. & CASTRICA, F. A Bioelectrical Sensor for the Detection of Small Biological Currents. 2010.
FAUMIA, H., ABIRAMI, B., MUTHULAKSHMI, K. & KASTHURI, M. 2014. A Knowledge Based Graphical Authentication Using X and Y Coordinates.
FENG, H.-H., LE, A. & SCANLON, J. 2013. *Detailed History* [Online]. Available: http://www.cs.gmu.edu/cne/itcore/security/timeline.html [Accessed 23/04/2015 2015].
FFIEC. 2002. *Authentication in an Internet Banking Environment* [Online]. Federal Financial Institutions Examination Council. [Accessed].
FISCHER, I. T., KUO, C., HUANG, L. & FRANK, M. Short paper: Smartphones: Not smart enough? Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices, 2012. ACM, 27-32.
FISTOFFURY. 2013. *Responsive Web Design & Mobile Marketing Trends* [Online]. Available: http://wearefury.com/ideas/responsive-web-design-mobile-marketing-trends/ [Accessed].
FLORENCIO, D. & HERLEY, C. A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*, 2007 Banff, Alberta, Canada.: International World Wide Web Conference Committee (IW3C2). 657-666.

FLORÊNCIO, D., HERLEY, C. & COSKUN, B. 2007. *Do strong web passwords accomplish anything?* [Online]. Available: https://www.usenix.org/legacy/event/hotsec07/tech/full_papers/florencio/florencio.pdf [Accessed].

FRANK, M. 2013. *Chaos Computer Club breaks Apple TouchID* [Online]. Chaos Computer Club. Available: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid [Accessed 24/06, 2015].

FRANK, M., BIEDERT, R., MA, E.-D., MARTINOVIC, I. & SONG, D. 2013. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *Information Forensics and Security, IEEE Transactions on,* 8**,** 136-148.

FUHRMAN, S., CUNNINGHAM, M. J., WEN, X., ZWEIGER, G., SEILHAMER, J. J. & SOMOGYI, R. 2000. The application of Shannon entropy in the identification of putative drug targets. *Biosystems,* 55**,** 5-14.

GAFUROV, D. 2010. *Emerging biometric modalities: challenges and opportunities*. *Security Technology, Disaster Recovery and Business Continuity.* Springer.

GAHI, Y., LAMRANI, M., ZOGLAT, A., GUENNOUN, M., KAPRALOS, B. & EL-KHATIB, K. Biometric identification system based on electrocardiogram data. New Technologies, Mobility and Security, 2008. NTMS'08., 2008. IEEE, 1-5.

GAUTAM, S. 2014. *What are the sales statistics for e-commerce?* [Online]. quora. Available: http://www.quora.com/What-are-the-sales-statistics-for-e-commerce [Accessed].

GEHALOT, P. 2013. *Designing a better authentication model.* Master of Science, San Diego State University.

GEIGER, J. T., HOFMANN, M., SCHULLER, B. & RIGOLL, G. Gait-based person identification by spectral, cepstral and energy-related audio features. Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on, 2013. IEEE, 458-462.

GEMALTO. 2009. *Gemalto Mobile Banking Services* [Online]. Available: http://www.mobile-money-gateway.com/sites/default/files/document/1/Gemalto%20Mobile%20Banking%20Services.pdf [Accessed 11/04/2015 2015].

GEMALTO. 2013. *Gartner recognizes growing importance of user authentication* [Online]. Available: http://blog.gemalto.com/blog/2013/04/02/gartner-recognizes-growing-importance-of-user-authentication/#sthash.qlWktuGV.dpuf [Accessed].

GEORGOULAS, G., CHUDACEK, V., RIEGER, J., STYLIOS, C. & LHOTSKA, L. METHODS AND TOOLS FOR PROCESSING BIOSIGNALS: A SURVEY PAPER. IFMBE Proc, 2005. 1727-1983.

GFI. 2009. *The dangers faced by your corporate network* [Online]. Available: http://www.gfi.com/whitepapers/cyber-attacks.pdf [Accessed 11/07/2014 2014].

GITHUB. 2017. *The State of the Octoverse 2017* [Online]. Available: https://octoverse.github.com/ [Accessed 30/03/2018].

GIVENS, G., BEVERIDGE, J. R., DRAPER, B. A., GROTHER, P. & PHILLIPS, P. J. How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on, 2004. IEEE, II-381-II-388 Vol. 2.

GLOBAL ANDUSTRY ANALYSTS, I. 2017. Access vis smartphones emerge as a key trend in the global electronic access control systems market. *Global Andustry Analysts, Inc*.

GOKHALE, M. & KHANDUJA, D. K. 2010. Time domain signal analysis using wavelet packet decomposition approach. *International Journal of Communications, Network and System Sciences,* 3**,** 321.

GOLLMAN, D. 2011. *Computer Security*, John Wiley & Sons.

GOMEZ, A., QUINTERO, L., LOPEZ, N. & CASTRO, J. An approach to emotion recognition in single-channel EEG signals: a mother child interaction. Journal of Physics: Conference Series, 2016. IOP Publishing, 012051.

GOUDA, M. G., LIU, A. X., LEUNG, L. M. & ALAM, M. A. 2015. Single password, multiple accounts. Austin, Texas 78712-0233, U.S.A: The University of Texas at Austin,.

GRAND, J. 2001. *Authentication Tokens: Balancing the Security Risks with Business Requirements* [Online]. Available: http://www.researchgate.net/publication/2487661_Authentication_Tokens_Balancing_the_Security_Risks_with_Business_Requirements [Accessed 12/11 2014].

GROTHER, P. & TABASSI, E. 2007. Performance of biometric quality measures. *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* 29**,** 531-543.

HACKETT, M. & HAWKEY, K. 2012. Security, privacy and usability requirements for federated identity. Available: http://www.w2spconf.com/2012/papers/w2sp12-final18.pdf.

HALLSTEINSEN, S. & JORSTAD, I. Using the mobile phone as a security token for unified authentication. Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on, 2007. IEEE, 68-68.

HAMMOND, J. & WHITE, P. 1996. The analysis of non-stationary signals using time-frequency methods. *Journal of Sound and Vibration,* 190**,** 419-447.

HAN, J. & BHANU, B. 2006. Individual recognition using gait energy image. *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* 28**,** 316-322.

HARRIERO, A., RAMOS, D., GONZALEZ-RODRIGUEZ, J. & FIERREZ, J. 2009. Analysis of the utility of classical and novel speech quality measures for speaker verification. *Advances in Biometrics*. Springer.

HE, C. & WANG, Z. J. An independent component analysis (ICA) based approach for EEG person authentication. Bioinformatics and Biomedical Engineering, 2009. ICBBE 2009. 3rd International Conference on, 2009. IEEE, 1-4.

HEMA, C. & ELAKKIYA, A. 2012. Recurrent Neural Network based Recognition of EEG Biographs.

HEMA, C. & OSMAN, A. Single trial analysis on EEG signatures to identify individuals. Signal Processing and Its Applications (CSPA), 2010 6th International Colloquium on, 2010. IEEE, 1-3.

HEMA, C. R., PAULRAJ, M. & KAUR, H. Brain signatures: a modality for biometric authentication. Electronic Design, 2008. ICED 2008. International Conference on, 2008. IEEE, 1-4.

HERI KUSWANTO, M. S. A. M. I. F. 2017. Random Forest Classification and Support Vector Machine for Detecting Epilepsyusing Electroencephalograph Records. *American Journal of Applied Sciences*

HISCOTT, R. 2013. *The Evolution of the Password — And Why It's Still Far From Safe* [Online]. Available: http://mashable.com/2013/12/30/history-of-the-password/ [Accessed].

HOLLINGWORTH, D. 2014. *Towords Threat, attack And Vulnerability taxonomies* [Online]. Available: http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/44/W1/02-Hollingworth.pdf [Accessed].

HOLZ, C., BUTHPITIYA, S. & KNAUST, M. Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body parts. Proceedings of the 33rd annual ACM conference on human factors in computing systems, 2015. ACM, 3011-3014.

HOUMANI, N., GARCIA-SALICETTI, S. & DORIZZI, B. A novel personal entropy measure confronted with online signature verification systems' performance. Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on, 2008. IEEE, 1-6.

HU, G.-S., ZHU, F.-F. & REN, Z. 2008. Power quality disturbance identification using wavelet packet energy entropy and weighted support vector machines. *Expert Systems with Applications,* 35**,** 143-149.

INDOVINA, M., ULUDAG, U., SNELICK, R., MINK, A. & JAIN, A. 2003. Multimodal biometric authentication methods: a COTS approach. *Proc. MMUA***,** 99-106.

INTELLIGENCE, B. 2017. *Mobile data will skyrocket 700% by 2021* [Online]. UK: BI Intelligence. [Accessed 13/04/2018 2018].

ISRAEL, S. A., IRVINE, J. M., CHENG, A., WIEDERHOLD, M. D. & WIEDERHOLD, B. K. 2005. ECG to identify individuals. *Pattern recognition,* 38**,** 133-142.

JAIN, A., HONG, L. & KULKARNI, Y. F2ID: A personal identification system using faces and fingerprints. Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on, 1998. IEEE, 1373-1375.

JAIN, A., HONG, L. & PANKANTI, S. 2000. Biometric identification. *Communications of the ACM,* 43**,** 90-98.

JAYAMAHA, R. M. M., SENADHEERA, M. R., GAMAGE, T. N. C., WEERASEKARA, K. P. B., DISSANAYAKA, G. & KODAGODA, G. N. Voizlock-human voice authentication system using hidden markov model. Information and Automation for Sustainability, 2008. ICIAFS 2008. 4th International Conference on, 2008. IEEE, 330-335.

JEONG, Y. 2011. Introduction to Bioelectricity. *Bio-Medical CMOS ICs.* Republic of Korea: Springer.

JOHNSON, D. B. & MALTZ, D. 1996. *Mobile computing*, Kluwer academic publishers Dordrecht.

JONES, V. M., IN'T VELD, R. H., TONIS, T., BULTS, R., VAN BEIJNUM, B., WIDYA, I., VOLLENBROEK-HUTTEN, M. & HERMENS, H. Biosignal and context monitoring: Distributed multimedia applications of body area networks in healthcare. Multimedia Signal Processing, 2008 IEEE 10th Workshop on, 2008. IEEE, 820-825.

JOSANG, A., ALFAYYADH, B., GRANDISON, T., ALZOMAI, M. & MCNAMARA, J. Security usability principles for vulnerability analysis and risk assessment. Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual, 2007. Ieee, 269-278.

JUST , M. 2014, p.1. Authentication Frequency as an Important Design Factor. *Symposium on Usable Privacy and Security (SOUPS)* [Online]. Available: http://cups.cs.cmu.edu/soups/2014/workshops/papers/frequency_just_15.pdf [Accessed 24/10].

KAGANOV, V., KOROLYOV, A., KRYLOV, M., MASHECHKIN, I. & PETROVSKIY, M. Hybrid method for active authentication using keystroke dynamics. Hybrid Intelligent Systems (HIS), 2014 14th International Conference on, 2014. IEEE, 61-66.

KAINDA, R., FLECHAIS, I. & ROSCOE, A. Security and usability: Analysis and evaluation. *International Conference on Availability, Reliability, and Security, ARES'10.*, 2010. IEEE, 275-282.

KALE, R., GORE, N., JADHAV, K. & SHINDE, M. S. 2013. Review Paper on Two Factor Authentication Using Mobile Phone (Android). *Journal of Computer Engineering and Informatics,* 1**,** 99-102.

KALKA, N. D., ZUO, J., SCHMID, N. A. & CUKIC, B. 2010. Estimating and fusing quality factors for iris biometric images. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on,* 40**,** 509-524.

KAUR, G. & VERMA, C. K. 2014. Comparative Analysis of Biometric Modalities. *International Journal of Advanced Research in Computer Science and Software Engineering,* 4**,** 603-613.

KAWAMOTO, H., TAAL, S., NINISS, H., HAYASHI, T., KAMIBAYASHI, K., EGUCHI, K. AND SANKAI, Y., 2010, August. Voluntary motion support control of Robot Suit HAL triggered by bioelectrical signal for hemiplegia. In *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE* (pp. 462-466). IEEE.

KELION, L. 2014. *Android Fake ID bug exposes smartphones and tablets* [Online]. Available: http://www.bbc.co.uk/news/technology-28544443 [Accessed 23/07 2014].

KHAKUREL, J., PÖYSÄ, S. & PORRAS, J. The Use of Wearable Devices in the Workplace-A Systematic Literature Review. International Conference on Smart Objects and Technologies for Social Good, 2016. Springer, 284-294.

KHAN, U. & ZAHID, H. 2010. COMPARATIVE STUDY OF AUTHENTICATION TECHNIQUES. *International Journal of Video & Image Processing & Network Security,* 10.

KIM, D.-J. & HONG, K.-S. 2008. Multimodal biometric authentication using teeth image and voice in mobile environment. *Consumer Electronics, IEEE Transactions on,* 54**,** 1790-1797.

KIM, K.-S., YOON, T.-H., LEE, J.-W., KIM, D.-J. & KOO, H.-S. A robust human identification by normalized time-domain features of electrocardiogram. Engineering in medicine and biology society, 2005. ieee-embs 2005. 27th annual international conference of the, 2006. IEEE, 1114-1117.

KISKU, D. R., GUPTA, P. & SING, J. K. 2009. Feature level fusion of biometrics cues: Human identification with Doddington's Caricature. *Security Technology*. Springer.

KOONG, C.-S., YANG, T.-I. & TSENG, C.-C. 2014. A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices. *The Scientific World Journal,* 2014.

KOUSARRIZI, M. N., TESHNEHLAB, M., ALIYARI, M. & GHARAVIRI, A. Feature extraction and classification of EEG signals using Wavelet transform, SVM and artificial neural networks for brain computer interfaces. Bioinformatics, Systems Biology and Intelligent Computing, 2009. IJCBS'09. International Joint Conference on, 2009. IEEE, 352-355.

KROL, K., PHILIPPOU, E., DE CRISTOFARO, E. & SASSE, M. A. 2015. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. *arXiv preprint arXiv:1501.04434*.

KRUPP, A., RATHGEB, C. & C.BUSCH 2013. Social Acceptance of Biometric Technologies in Germany: A Survey. University of Applied Sciences Darmstadt, Germany: Biometrics and Internet Security Research Group.

LAINE, A. & FAN, J. 1993. Texture classification by wavelet packet signatures. *IEEE Transactions on pattern analysis and machine intelligence,* 15**,** 1186-1191.

LAU, L. 2016. Wavelet packets based denoising method for measurement domain repeat-time multipath filtering in GPS static high-precision positioning. *GPS Solutions,* 2**,** 461-474.

LAWRENCE, D. 2014. *Google's Android Has a Fake-ID Problem* [Online]. Available: http://www.bloomberg.com/bw/articles/2014-07-29/googles-android-has-a-fake-id-problem [Accessed 17 Febuary 2015].

LEE, J., CHEE, Y. & KIM, I. 2012. Personal identification based on vectorcardiogram derived from limb leads electrocardiogram. *Journal of Applied Mathematics,* 2012**,**
.

LEE, Y.-Y. & HSIEH, S. 2014. Classifying different emotional states by means of EEG-based functional connectivity patterns. *PloS one,* 9**,** e95415.

LI, F., CLARKE, N., PAPADAKI, M. & DOWLAND, P. Behaviour Profiling for Transparent Authentication for Mobile Devices. Emerging Security Technologies (EST), 2010 International Conference on, 2010. IEEE, 77-82.

LIAW, A. & WIENER, M. 2002. Classification and regression by randomForest. R News, 2 (3): 18–22. R package version 4.6. 10.

LIM, S. Y., KIAH, M. M. & ANG, T. F. 2017. Security Issues and Future Challenges of Cloud Service Authentication. *Acta Polytechnica Hungarica,* 14**,** 69-89.

LIN, C.-C., CHANG, C.-C. & LIANG, D. A Novel Non-intrusive User Authentication Method Based on Touchscreen of Smartphones. Biometrics and Security Technologies (ISBAST), 2013 International Symposium on, 2013. IEEE, 212-216.

MALEMPATI, S. & MOGALLA, S. 2011 An Ancient Indian Board Game as a Tool for Authentication *International Journal of Network Security & Its Applications (IJNSA),* 3**,** 149-160.

MALLAT, S. G. 1989. A theory for multiresolution signal decomposition: the wavelet representation. *IEEE transactions on pattern analysis and machine intelligence,* 11**,** 674-693.

MANSFIELD, A. & WAYMAN, J. 2002. Best Practices in Testing and Reporting Performance of Biometric Devices.

MANSFIELD, T. 1999. BIOMETRICS: A TECHNICAL PRIMER.

MARTINEZ-DIAZ, M., FIERREZ, J., GALBALLY, J., ALONSO-FERNANDEZ, F. & ORTEGA-GARCIA, J. 2007. Signature Verification on Handheld Devices.

MATHER, A. T. 2013. *Expect More Growth* [Online]. Houston, Tex: security-today. Available: http://security-today.com/Articles/2013/12/01/Expect-More-Growth.aspx?Page=3 [Accessed Dec 01 2015].
MCGREGOR, J. 2014. *The Top 5 Most Brutal Cyber Attacks Of 2014 So Far* [Online]. Available: http://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far/ [Accessed 05/05 2015].
MCKEE, J. 2014. *HSBC Opens Paym Capabilities to Business Customers* [Online]. Daily Insight Available: http://maps.yankeegroup.com/ygapp/content/8f7fd65fa50e4ef38255cf2b5ef726a0/51/DAILYINSIGHT/0 [Accessed 11/04 2015].
MICROSOFT. 2018. *Microsoft Health*
[Online]. Available: https://www.microsoft.com/en-us/microsoft-health [Accessed 2018].
MICULAN, M. & URBAN, C. 2011. Formal analysis of Facebook Connect single sign-on authentication protocol.
MINTO, R. 2012. *EM e-commerce: growing unequally* [Online]. beyondbrics. Available: http://blogs.ft.com/beyond-brics/2012/03/19/em-e-commerce-growing-unequally/ [Accessed 11/03 2015].
MOHANCHANDRA, K., LINGARAJU, G., KAMBLI, P. & KRISHNAMURTHY, V. 2013. Using brain waves as new biometric feature for authenticating a computer user in real-time. *International Journal of Biometrics and Bioinformatics (IJBB),* 7**,** 49.
MORGAN, L. 2014. *List of cyber attacks and data breaches in 2014* [Online]. Available: http://www.itgovernance.co.uk/blog/list-of-the-hacks-and-breaches-in-2014/ [Accessed 2015].
MORRISON, W. 2013 Wearable Devices and the Future of Two Factor Authentication. Available from: https://www.logintc.com/blog/2013-12-18-wearable-devices-and-authentication.html.
MOUKADEM, A., ABDESLAM, D. O. & DIETERLEN, A. 2014. *Time-Frequency Domain for Segmentation and Classification of Non-stationary Signals: The Stockwell Transform Applied on Bio-signals and Electric Signals*, John Wiley & Sons.
MURPHY, C. 2011. Cellular Phone Evidence Data Extraction and Documentation.
NAFIS, N. A review on the Existent and Emerging Biometrics Modalities. Advances in Electrical & Information Communication Technology, AEICT-2014, 2014 Uttar Pradesh Technical University, India. Department of Electronics & communication Engineering PSIT, 416-421.
NAG, A. K., DASGUPTA, D. & DEB, K. An Adaptive Approach for Active Multi-Factor Authentication. 9th Annual Symposium on Information Assurance (ASIA'14), 2014. 39.
NANDAKUMAR, K., ROSS, A. & JAIN, A. K. Biometric fusion: does modeling correlation really matter? Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on, 2009. IEEE, 1-6.
NANDISH, M., STAFFORD, M., KUMAR, P. & AHMED, F. 2012. Feature Extraction and Classification of EEG Signal Using Neural Network Based Techniques. *International Journal of Engineering and Innovative Technology (IJEIT) Volume,* 2.
NANEHKARAN, Y. A. 2013. An Introduction To Electronic Commerce.
NEMOTO, T., FURUKAWA, K. & OKAMOTO, M. 2011. Poster: Knowledge-Based Authentication using Twitter.
NICKEL, C., BRANDT, H. & BUSCH, C. 2011. Classification of Acceleration Data for Biometric Gait Recognition on Mobile Devices. *Biosig,* 11**,** 57-66.
NIRANJANAMURTHY, M. & CHAHAR, D. D. 2013. The study of e-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering,* 2.
PAL, A., GAUTAM, A. K. & SINGH, Y. N. 2015. Evaluation of Bioelectric Signals for Human Recognition. *Procedia Computer Science,* 48**,** 747-753.
Pancrazio, J.J., Bey Jr, P.P., Loloee, A., Manne, S., Chao, H.C., Howard, L.L., Gosney, W.M., Borkholder, D.A., Kovacs, G.T., Manos, P. and Cuttino, D.S., 1998. Description and

demonstration of a CMOS amplifier-based-system with measurement and stimulation capability for bioelectrical signal transduction. *Biosensors and Bioelectronics*, *13*(9), pp.971-979.
PARAK, J. & KORHONEN, I. Evaluation of wearable consumer heart rate monitors based on photopletysmography. Engineering in Medicine and Biology Society (EMBC), 2014 36th Annual International Conference of the IEEE, 2014. IEEE, 3670-3673.
PATEL, S., PARK, H., BONATO, P., CHAN, L. & RODGERS, M. 2012. A review of wearable sensors and systems with application in rehabilitation. *Journal of neuroengineering and rehabilitation,* 9**,** 21.
PATIL, K. I. & SHIMPI, J. 2013. A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*2.
PAYM 2015. £26m Already Transferred Via Paym in 2014. *Mobile Payments Service Company Limited*.
PEREZ, J. C. 2005. *Gartner: Security concerns to stunt e-commerce growth* [Online]. IDG News Service Available: http://www.computerworld.com/article/2558007/e-commerce/gartner--security-concerns-to-stunt-e-commerce-growth.html [Accessed 4/08 2014].
PHILLIPS, P. J., MARTIN, A., WILSON, C. L. & PRZYBOCKI, M. 2000. An introduction evaluating biometric systems. *Computer,* 33**,** 56-63.
PINOLA, M. 2012. *How Often Should I Change My Passwords?* [Online]. Available: http://lifehacker.com/5966214/how-often-should-i-change-my-passwords [Accessed 23/4 2015].
PRNEWSWIRE. 22 Oct, 2014 2014. Electronic Access Control Systems Market is Expected to Reach USD 31.2 Billion Globally in 2019: Transparency Market Research. Available from: http://www.prnewswire.co.uk/news-releases/electronic-access-control-systems-market-is-expected-to-reach-usd-312-billion-globally-in-2019-transparency-market-research-266057071.html.
PROCESSOR, P. I. M. 2017. *Companion for Microsoft Band* [Online]. Available: https://apkpure.com/companion-for-microsoft-band/com.pimp.companionforband [Accessed 2017-09-20 2017].
PWC. 2015. *Cyber security: Building confidence in your digital future* [Online]. Available: http://www.pwc.co.uk/cyber-security/cyber-security.jhtml [Accessed 02/02 2015].
RAO, T. V. N. & VEDAVATHI, K. 2011. Authentication Using Mobile Phone as a Security Token. *International Journal of Computer Science & Engineering Technology (IJCSET),* 1**,** 569-574.
REISS, A. & STRICKER, D. Introducing a new benchmarked dataset for activity monitoring. Wearable Computers (ISWC), 2012 16th International Symposium on, 2012. IEEE, 108-109.
RÍHA, Z. K. & MATYÁŠ, V. 2000. *Biometric Authentication Systems*. Masaryk University.
RILA, L. & MITCHELL, C. J. Security protocols for biometrics-based cardholder authentication in smartcards. Applied Cryptography and Network Security, 2003. Springer, 254-264.
RITCHIE, R., RUBINO, D., MICHALUK, K. & NICKINSON, P. 2014. The future of authentication: Biometrics, multi-factor, and co-dependency.
RIVA, O., QIN, C., STRAUSS, K. & LYMBEROPOULOS, D. Progressive Authentication: Deciding When to Authenticate on Mobile Phones. 2012.
RNMO, L. S. & LAGUNA, P. 2006. Electrocardiogram (ecg) signal processing.
RODWELL, P., FURNELL, S. & REYNOLDS, P. L. 2007. A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers & Security,* 26**,** 468-478.
ROSS, A. & JAIN, A. 2004. *Multimodal biometrics: An overview*, na.
ROTH, J., LIU, X. & METAXAS, D. 2014. On continuous user authentication via typing behavior.
SAEVANEE, H. 2014. Continuous User Authentication Using Multi-Modal Biometrics.
SAEVANEE, H., CLARKE, N., FURNELL, S. & BISCIONE, V. 2015. Continuous user authentication using multi-modal biometrics. *computers & security,* 53**,** 234-246.

SAFARA, F., DORAISAMY, S., AZMAN, A., JANTAN, A. & RAMAIAH, A. R. A. 2013. Multi-level basis selection of wavelet packet decomposition tree for heart sound classification. *Computers in biology and medicine,* 43**,** 1407-1414.
SAINI, R. & RANA, N. 2014. Comparison of Various Biometric Methods. *International Journal of Advances in Science and Technology (IJAST),* 2.
SANCHO, J., ALESANCO, A. & GARCIA, J. 2018. Biometric Authentication Using the PPG: A Long-Term Feasibility Study. *Sensors (Basel, Switzerland),* 18.
SASIKALA, P. & WAHIDABANU, R. 2010. Identification of individuals using electrocardiogram. *International journal of computer science and network security,* 10**,** 147-153.
SASIKALA, P. & WAHIDAUANU, R. 2010. Identification of individuals using electrocardiogram. *International Journal of Computer Science and Network Security,* 10**,** 147-153.
SASSE, M. A. 2005. *Usability and trust in information systems* [Online]. Available: http://discovery.ucl.ac.uk/20346/2/forsight.pdf [Accessed 27/08 2014].
SATHISH, S., JOSHI, A. B. & SHIDAGANTI, G. I. 2013 User Authentication Methods and Techniques by Graphical Password: A Survey. *International Journal of Computer Applications & Information Technology,* Vol. 2.
SCHEIDAT, T., ENGEL, A. & VIELHAUER, C. Parameter optimization for biometric fingerprint recognition using genetic algorithms. Proceedings of the 8th Workshop on Multimedia and Security, 2006. ACM, 130-134.
SCHMIDT, A., AIDOO, K. A., TAKALUOMA, A., TUOMELA, U., VAN LAERHOVEN, K. & VAN DE VELDE, W. Advanced interaction in context. International Symposium on Handheld and Ubiquitous Computing, 1999. Springer, 89-101.
SCHULTZ, E. E., PROCTOR, R. W., LIEN, M.-C. & SALVENDY, G. 2001. Usability and security an appraisal of usability issues in information security methods. *Computers & Security,* 20**,** 620-634.
SCOTT, M. 2014. *A Brief History of Authentication* [Online]. Available: https://www.certivox.com/blog/a-brief-history-of-authentication [Accessed 2/05 2014].
SETHI, A., MANZOOR, O. & SETHI, T. 2011. *User Authentication on Mobile Devices* [Online]. Available: http://www.cigital.com/wp-content/uploads/downloads/2012/11/mobile-authentication.pdf [Accessed].
SHAIKH, A. A. & KARJALUOTO, H. 2015. Mobile banking adoption: A literature review. *Telematics and Informatics,* 32**,** 129-142.
SHEN, C., CAI, Z., GUAN, X., DU, Y. & MAXION, R. A. 2013. User authentication through mouse dynamics. *IEEE Transactions on Information Forensics and Security,* 8**,** 16-30.
SHEN, T.-W. 2005. *Biometric identity verification based on electrocardiogram (ECG)*, University of Wisconsin--Madison.
SIDEK, K. A. & KHALIL, I. Automobile driver recognition under different physiological conditions using the electrocardiogram. 2011 Computing in Cardiology, 2011a. IEEE, 753-756.
SIDEK, K. A. & KHALIL, I. Automobile driver recognition under different physiological conditions using the electrocardiogram. Computing in Cardiology, 2011, 2011b. IEEE, 753-756.
SIN, D., LAWSON, E. & KANNOORPATTI, K. Mobile Web Apps-The Non-programmer's Alternative to Native Applications. Human System Interactions (HSI), 2012 5th International Conference on, 2012. IEEE, 8-15.
SINGH, P. I. & THAKUR, G. S. M. 2012. Enhanced Password Based Security System Based on User Behavior using Neural Networks *I.J. Information Engineering and Electronic Business***,** 29-35
SRIYANANDA, H., TOWILL, D. & WILLIAMS, J. 1975. Voting Techniques for Fault diagnosis from frequency-domain test-data. *IEEE Transactions on Reliability,* 24**,** 260-267.
STAJANO, F. 2011. Pico: No more passwords! *Security Protocols XIX.* Springer.
STATISTA 2018. Percentage of all global web pages served to mobile phones from 2009 to 2018. *The Statistics Portal*.

STATISTA, T. 2015. *The Statistics Portal* [Online]. Available: http://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/ [Accessed 11/03 2015].

STEPHEN, M. J. & REDDY, P. P. 2011. Implementation of Easy Fingerprint Image Authentication with Traditional Euclidean and Singular Value Decomposition Algorithms. *Int. J. Advance. Soft Comput. Appl,* 3.

SUBASI, A. 2007. EEG signal classification using wavelet feature extraction and a mixture of expert model. *Expert Systems with Applications,* 32**,** 1084-1093.

TAKADA, T. & KOIKE, H. 2003. A wase-E: Authentication for mobile phones using user's favourite images. *5th International Symposium, Mobile HCI 2003.* Human-Computer Interaction with Mobile Devices and Services

TAMIL, E. B. M., KAMARUDIN, N., SALLEH, R. & TAMIL, A. A review on feature extraction & classification techniques for biosignal processing (Part I: Electrocardiogram). 4th Kuala Lumpur International Conference on Biomedical Engineering 2008, 2008. Springer, 107-112.

TANG, Y., HIDENORI, N. & URANO, Y. User authentication on smart phones using a data mining method. Information Society (i-Society), 2010 International Conference on, 2010. IEEE, 173-178.

TANVI, P., SONAL, G. & KUMAR, S. M. Token Based Authentication using Mobile Phone. 2011 International Conference on Communication Systems and Network Technologies, 2011. 85-88.

TARASEWICH, P. 2003. Designing mobile commerce applications. *Communications of the ACM,* 46**,** 57-60.

TAWFIK, M. M. & KAMAL, H. S. T. 2011. Human identification using QT signal and QRS complex of the ECG. *Online J. Electron. Elect. Eng,* 3**,** 383-387.

TECHNOLOGIES, W. 2013. *GADGET OF THE MONTH* [Online]. Available: http://www.wearable-technologies.com/gadgets-of-the-month/phyode-wme-smart-wristband [Accessed].

TECHNOLOJ 2017 Mobile Payment Trends to Watch out for in 2017. *lets talk payments*.

TEPLAN, M. 2002. Fundamentals of EEG measurement. *Measurement science review,* 2**,** 1-11.

THIEMERT, S., SAHBI, H. & STEINEBACH, M. Using entropy for image and video authentication watermarks. Security, Steganography, and Watermarking of Multimedia Contents VIII, 2006. International Society for Optics and Photonics, 607218.

TODOROV, D. 2007. *Mechanics of user identification and authentication: Fundamentals of identity management*, CRC Press.

TODORVOV, D. 2007. *Mechanics of User Identification and Authentication:Fundamentals of Identity Managemen*, Auerbach Publications.

TRANSPARENCYMARKETRESEARCH. 2014. Electronic Access Control Systems Market Global Forecast, Market Share, Size, Growth and Industry Analysis, 2014 - 2019. Available: http://www.transparencymarketresearch.com/electronic-access-control.html.

TRESADERN, P., COOTES, T. F., POH, N., MATEJKA, P., HADID, A., LEVY, C., MCCOOL, C. & MARCEL, S. 2013. Mobile biometrics: Combined face and voice verification for a mobile platform. *IEEE pervasive computing***,** 79-87.

TRICOCHE, X., MACLEOD, R. & JOHNSON, C. R. 2008. Visual Analysis of Bioelectric Fields. *Visualization in Medicine and Life Sciences.* Springer.

TRIPATHI, K. 2011. A comparative study of biometric technologies with reference to human interface.

TSAI, S.-J. S. 2002. Power transformer partial discharge (PD) acoustic signal detection using fiber sensors and wavelet analysis, modeling, and simulation.

TULYAKOV, S., JAEGER, S., GOVINDARAJU, V. & DOERMANN, D. 2008. Review of classifier combination methods. *Machine learning in document analysis and recognition.* Springer.

TUYTELAARS, T. & MIKOLAJCZYK, K. 2008. Local invariant feature detectors: a survey. *Foundations and trends® in computer graphics and vision,* 3**,** 177-280.

VAN DER HORST, T. W. & SEAMONS, K. E. Simple authentication for the web. Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on, 2007. IEEE, 473-482.
VARANIS, M. & PEDERIVA, R. 2015. Wavelet Packet Energy-Entropy Feature Extraction and Principal Component Analysis for Signal Classification. *Proceeding Series of the Brazilian Society of Computational and Applied Mathematics,* 3.
VARCHOL, P. & LEVICKY, D. 2007. Using of Hand Geometry in Biometric Security Systems. *RADIOENGINEERING REVIEWERS,* 16**,** 82-87.
VASIETE, E., CHEN, Y., PATEL, V., DAVIS, L., CHAR, I., CHELLAPPA, R. & YEH, T. 2014. *Toward a Non-Intrusive, Physio-Behavioral Biometric for Smartphones* [Online]. Toronto, ON, Canada: MobileHCI '14,. Available: http://dx.doi.org/10.1145/2628363.2634223 [Accessed].
VENKATARAMANI, K., QIDWAI, S. & VIJAYAKUMAR, B. 2005. Face authentication from cell phone camera images with illumination and temporal variations. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* 35**,** 411-418.
WALLACE, S., CLARK, M. & WHITE, J. 2012. 'It's on my iPhone': attitudes to the use of mobile computing devices in medical education, a mixed-methods study. *BMJ open,* 2**,** e001099.
WANG, G., YU, J. & XIE, Q. 2013. Security analysis of a single sign-on mechanism for distributed computer networks. *IEEE Transactions on Industrial Informatics,* 9**,** 294-302.
WANG, R., CHEN, S. & WANG, X. Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services. Security and Privacy (SP), 2012 IEEE Symposium on, 2012. IEEE, 365-379.
WANG, Y., AGRAFIOTI, F., HATZINAKOS, D. & PLATANIOTIS, K. N. 2008. Analysis of human electrocardiogram for biometric recognition. *EURASIP journal on Advances in Signal Processing,* 2008**,** 19.
WANKHEDE, S. B. & VERMA, S. 2014. Keystroke dynamics authentication system using neural network. *International Journal of Innovative Research and Development,* 3.
WAYMAN, J., JAIN, A., MALTONI, D. & MAIO, D. 2005. An introduction to biometric authentication systems. *Biometric Systems.* Springer.
WEBER, H. 2012. *Facebook and Google dominate 76% of social logins, according to Janrain study* [Online]. Available: http://thenextweb.com/socialmedia/2012/05/04/facebook-and-google-dominate-76-of-social-logins-according-to-janrain-study/ [Accessed 11/04 2015].
WEICHENG, S. & KHANNA, R. 1997. Prolog To Evaluation Of Automated Biometrics-based Identification And Verification Systems. *Proceedings of the IEEE,* 85**,** 1463-1463.
WEICHENG, S., SURETTE, M. & KHANNA, R. 1997. Evaluation of automated biometrics-based identification and verification systems. *Proceedings of the IEEE,* 85**,** 1464-1478.
WEIR, C. S., DOUGLAS, G., CARRUTHERS, M. & JACK, M. 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security,* 28**,** 47-62.
WELCH, C. 2014. *Facebook will let users log into third-party apps anonymously* [Online]. the verge. Available: http://www.theverge.com/2014/4/30/5668750/facebook-announces-anonymous-login [Accessed 23/03/2015 2014].
WINFRASOFT. 2014. *Grid Pattern Authentication -Secure and simple* [Online]. Available: http://www.winfrasoft.com/media/documents/datasheets/Winfrasoft-AuthCentral-PINgrid-Datasheet.pdf [Accessed 19 November 2014].
WRIGHT, A. 2009. The magazine archive includes every article published in Communications of the ACM for over the past 50 years. *Communications of the ACM,* 54**,** 20-22.
XIAOMIN, W., TAIHUA, X. & WENFANG, Z. 2011. Chaos-based biometrics template protection and secure authentication. *In:* YANG, J. & NANNI, L. (eds.) *State of the art in Biometrics.* InTech.
YAZDANIFARD, R., HOE, F. K., ISLAM, M. R. & EMAMI, S. P. Customer's information security management system in E-commerce. of the2011 International Conference on Software and Computer Applications IPCSIT, 2011. 187-191.

YE, C., COIMBRA, M. T. & KUMAR, B. Investigation of human identification using two-lead electrocardiogram (ECG) signals. Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, 2010. IEEE, 1-8.

ZARGARZADEH, M. & MAGHOOLI, K. 2013. A behavioral biometric authentication system based on memory game.

ZHAO, Y., QIU, Z., YANG, Y., LI, W. & FAN, M. 2017. An empirical study of touch-based authentication methods on smartwatches. *arXiv preprint arXiv:1710.04608*.

ZHIWEI, L. & MINFEN, S. Classification of mental task EEG signals using wavelet packet entropy and SVM. Electronic Measurement and Instruments, 2007. ICEMI'07. 8th International Conference on, 2007. IEEE, 3-906-3-909.

ZIBRAN, M. F. 2012. *Biometric Authentication: The Security Issues* [Online]. Available: http://www.cs.usask.ca/documents/techreports/2012/TR-2012-02.pdf [Accessed 12/09 2014].

ZIN, A. N. M. & YUNOS, Z. 2005. *How to make online banking secure* [Online]. star-techcentral.com. Available: http://www.crime-research.org/analytics/online_banking/ [Accessed 27/07 2014].

ZOKAEE, S. & FAEZ, K. 2012a. Human identification based on ECG and palmprint. *International Journal of Electrical and Computer Engineering,* 2**,** 261.

ZOKAEE, S. & FAEZ, K. 2012b. Human identification based on ECG and palmprint. *International Journal of Electrical and Computer Engineering (IJECE),* 2**,** 261-266.

ZOLNA, R. 2016. *Putting a Finger on Our Phone Obsession Mobile touches: a study on humans and their tech* [Online]. Available: https://blog.dscout.com/mobile-touches [Accessed 31/01/2018 2018].

ZUEV, Y. A. & IVANOV, S. 1999. The voting as a way to increase the decision reliability. *Journal of the Franklin Institute,* 336**,** 361-378.

Appendix B: Ethical Approval, Consent Form and Information Sheet

RESEARCH WITH PLYMOUTH UNIVERSITY

11 January 2017

CONFIDENTIAL
Timibloudi Enamamu
School of Computing, Electronics and Mathematics

Dear Timibloudi

Amendment to Approved Application

***Application Title:** Bioelectrical User Authentication*

Thank you for your amended application addressing the conditions of your approval given by the Committee on 13 May 2016 and for informing the Committee of your revised dates for ethical approval from 10 November 2016 – 30 February 2017. I am pleased to confirm that this has been approved.

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Nathan Clarke

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

T +44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Jayne Brenen
Head of Faculty Operations

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENVIRONMENT

Human Ethics Committee Consent Form

CONSENT TO PARICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Timibloudi Enamamu

Title of Research

Bioelectrical User Authentication

Brief statement of purpose of work

The usability of a system is noticed from the first point of contact of that system more especially if the system is intrusive in perform a task. The usability of a user authentication system should address some key issues which include intrusiveness and user's ability to easily remember user login details. If these issues are met, it will greatly improve the authentication usage

This research seeks to meet these issues by using bioelectrical signals from a wearable device to overcome intrusiveness and avoid user's ability to know when authentication is done. To use bioelectrical signals for user authentication, it has to meet the basic requirement and characteristics needed to create a pattern for user authentication

This study will install software in your mobile phone for data extraction from the smart watch. As a participant, no modification will be made upon your mobile device before, during and after the collection of data. Please merely use your mobile phone as you normally do while the data will be continuously extracted during the two weeks duration. Also, a specified exercise of not more than 30 minutes with is done at the beginning and at the end of the data collection. Based upon Plymouth University guidelines, collected data should be stored for ten years. Upon the completion of the ten-year period, the collected data will be securely destroyed.

At all stages of the study, confidentiality of the collected data and subsequent analysis will be maintained. At no time, will any identifying information about the participants be used in any publication or research output.

You have the right to withdraw at any stage upon until the completion of the data collection process. Should you wish to withdraw from the study, please contact Timibloudi Enamamu. Moreover, declining participation and/or asking to withdraw from this study will not affect your study or your relationship with your supervisors or tutors.
For information regarding the study, please contact:

Timibloudi Enamamu – timibloudi.enamamu@plymouth.ac.uk

For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

---

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations)

Under these circumstances, I agree to participate in the research.

Name: ……..

Signature: …….. Date: ……..

SAMPLE INFORMATION SHEET FOR ADULT / CHILD

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENVIRONMENT

RESEARCH INFORMATION SHEET

Name of Principal Investigator

Timibloudi Enamamu

Title of Research

Bioelectrical User Authentication

Aim of research

1. To investigate the possibility of usage of bioelectrical signal to authenticate a user of a mobile device
2. To used user acceleration and orientation data to identify a user behaviour

Description of procedure

Three bioelectrical signals and an acceleration and orientation data will be extracted from each subject as the participants wear the smart watch.

Participants will not need to do anything other than to wear the smart watch which will be connected the participant's mobile phone. The data will be collected over a 2 weeks period.

Description of risks

All data collected will not be associated with any individual. Each participant name will be not be used at any point in time before, during and after collection of data

Benefits of proposed research

The research will provide an insight into the usability of bioelectrical signal for access control mechanism in a mobile device. The use of bioelectrical signal for access control mechanism will help reduce the human participation in the authentication process.

Right to withdraw

You have the right to withdraw at any stage. Your data and psychological profile will be removed and securely deleted. Also, declining participation and/or asking to withdraw from this study should not affect your PhD progression or your relationship with your supervisors.

Faculty of Science and Environment Ethical Application Form PS 2013/14 Final v.1

If you are dissatisfied with the way the research is conducted, please contact the principal investigator in the first instance: telephone number +441752586226. If you feel the problem has not been resolved please contact the secretary to the Faculty of Science and Environment Human Ethics Committee: Mrs Paula Simson 01752 584503.

Appendix C: Feature Extraction MATLAB Code

```
clear
load ('Exp1.mat');


def=Exp1;

for i=1:1800   %num of cols of a user
    for j=1:60   % num of rolls of user
        temp{j,i}= def (j,i);
    end
sig=cell2mat(temp(:,i));
% Calculation of low pass and high pass filter coefficients
[ld,hd]=wfilters('bior 4.4','d');
% First level decomposition
[a1,d1]=dwt(sig,ld,hd,'mode','per');

% Second level decomposition
[a2,d2]=dwt(d1,ld,hd,'mode','per');
% Third level decomposition
[a3,d3]=dwt(d2,ld,hd,'mode','per');

% Fourth level decomposition
[a4,d4]=dwt(d3,ld,hd,'mode','per');


% Calculation of features for 1st level detail coefficients
V1=var(d1);
Me1=(sum(d1.*d1)/length(d1));
MAXa1=max(d1);
MINa1=min(d1);
MAXe1=max(d1.*d1);
MINe1=min(d1.*d1);
STD1=std(d1);
Rang1=range(d1);
PEAK1=peak2peak(d1);
MAD1= mad(d1);
P2RM1 = peak2rms(d1);
RMs1 = rms(d1);

% Calculation of features for 2nd level detail coefficients
V2=var(d2);
Me2=(sum(d2.*d2)/length(d2));
MAXa2=max(d2);
MINa2=min(d2);
MAXe2=max(d2.*d2);
MINe2=min(d2.*d2);
STD2=std(d2);
```

```
Rang2=range(d2);
PEAK2=peak2peak(d2);
MAD2= mad(d2);
P2RM2 = peak2rms(d2);
RMs2 = rms(d2);


% Calculation of features for 3rd level detail coefficients
V3=var(d3);
Me3=(sum(d3.*d3)/length(d3));
MAXa3=max(d3);
MINa3=min(d3);
MAXe3=max(d3.*d3);
MINe3=min(d3.*d3);
STD3=std(d3);
Rang3=range(d3);
PEAK3=peak2peak(d3);
MAD3= mad(d3);
P2RM3 = peak2rms(d3);
RMs3 = rms(d3);


% Calculation of features for 4th level detail coefficients
V4=var(d4);
Me4=(sum(d4.*d4)/length(d4));
MAXa4=max(d4);
MINa4=min(d4);
MAXe4=max(d4.*d4);
MINe4=min(d4.*d4);
STD4=std(d4);
Rang4=range(d4);
PEAK4=peak2peak(d4);
MAD4= mad(d4);
P2RM4 = peak2rms(d4);
RMs4 = rms(d4);


% Calculation of features 4th level approximation coefficients
V5=var(a4);
Me5=(sum(a4.*a4)/length(a4));
MAXa5=max(a4);
MINa5=min(a4);
MAXe5=max(a4.*a4);
MINe5=min(a4.*a4);
STD5=std(a4);
Rang5=range(a4);
PEAK5=peak2peak(a4);
MAD5= mad(a4);
P2RM5= peak2rms(d4);
```

```
RMs5 = rms(d4);


% Proper display and alignment statements
VAR=[V1,V2,V3,V4,V5];
MEANe=[Me1,Me2,Me3,Me4,Me5];
MAXa=[MAXa1,MAXa2,MAXa3,MAXa4,MAXa5];
MINa=[MINa1,MINa2,MINa3,MINa4,MINa5];
MAXe=[MAXe1,MAXe2,MAXe3,MAXe4,MAXe5];
MINe=[MINe1,MINe2,MINe3,MINe4,MINe5];
STD=[STD1,STD2,STD3,STD4,STD5];
Rang=[Rang1,Rang2,Rang3,Rang4,Rang5];
PEAK2p=[PEAK1,PEAK2,PEAK3,PEAK4,PEAK5];
MADiv=[MAD1,MAD2, MAD3,MAD4,MAD5];
P2rm=[P2RM1,P2RM2,P2RM3,P2RM4,P2RM5];
Rms =[RMs1,RMs2,RMs3,RMs4,RMs5];



Output_BioelecFeat{1,i}=V1;
Output_BioelecFeat{2,i}=Me1;
Output_BioelecFeat{3,i}=MAXa1;
Output_BioelecFeat{4,i}=MINa1;
Output_BioelecFeat{5,i}=MAXe1;
Output_BioelecFeat{6,i}=MINe1;
Output_BioelecFeat{7,i}=STD1;
Output_BioelecFeat{8,i}=Rang1;
Output_BioelecFeat{9,i}=PEAK1;
Output_BioelecFeat{10,i}=MAD1 ;
Output_BioelecFeat{11,i}=P2RM1;
Output_BioelecFeat{12,i}=RMs1;

Output_BioelecFeat{13,i}=V2;
Output_BioelecFeat{14,i}=Me2;
Output_BioelecFeat{15,i}=MAXa2;
Output_BioelecFeat{16,i}=MINa2;
Output_BioelecFeat{17,i}=MAXe2;
Output_BioelecFeat{18,i}=MINe2;
Output_BioelecFeat{19,i}=STD2;
Output_BioelecFeat{20,i}=Rang2;
Output_BioelecFeat{21,i}=PEAK2;
Output_BioelecFeat{22,i}= MAD2 ;
Output_BioelecFeat{23,i}=P2RM2;
Output_BioelecFeat{24,i}=RMs2;



Output_BioelecFeat{25,i}=V3;
Output_BioelecFeat{26,i}=Me3;
Output_BioelecFeat{27,i}=MAXa3;
Output_BioelecFeat{28,i}=MINa3;
```

```
Output_BioelecFeat{29,i}=MAXe3;
Output_BioelecFeat{30,i}=MINe3;
Output_BioelecFeat{31,i}=STD3;
Output_BioelecFeat{32,i}=Rang3;
Output_BioelecFeat{33,i}=PEAK3;
Output_BioelecFeat{34,i}= MAD3 ;
Output_BioelecFeat{35,i}=P2RM3;
Output_BioelecFeat{36,i}=RMs3;


Output_BioelecFeat{37,i}=V4;
Output_BioelecFeat{38,i}=Me4;
Output_BioelecFeat{39,i}=MAXa4;
Output_BioelecFeat{40,i}=MINa4;
Output_BioelecFeat{41,i}=MAXe4;
Output_BioelecFeat{42,i}=MINe4;
Output_BioelecFeat{43,i}=STD4;
Output_BioelecFeat{44,i}=Rang4;
Output_BioelecFeat{45,i}=PEAK4;
Output_BioelecFeat{46,i}= MAD4 ;
Output_BioelecFeat{47,i}=P2RM4;
Output_BioelecFeat{48,i}=RMs4;


end
```